HACKING SEBAGAI FENOMENA CYBERCRIME

(Kajian Kriminologis Terhadap Fenomena Hacker Di Cyberspace)

T E S I S

Disusun Dalam Rangka Memenuhi Persyaratan
Program Magister Ilmu Hukum

Oleh:
AGUS RAHARJO
B4A099007

Pembimbing
Prof. Dr I.S. SUSANTO, S.H.

PROGRAM MAGISTER ILMU HUKUM
UNIVERSITAS DIPONEGORO
SEMARANG
2001

HACKING SEBAGAI FENOMENA CYBERCRIME

(Kajian Kriminologis Terhadap Fenomena Hacker Di Cyberspace)

Disusun oleh

AGUS RAHARJO

B4A099007

Dipertahankan di depan Dewan Penguji

Pada tanggal 13-14 Agustus 2001

Tesis ini telah diterima

Sebagai persyaratan untuk memperoleh gelar

Magister Ilmu Hukum

Mengetahui,

Pembimbing,

Prof. Dr I.S. Susanto, S.H.

Ketua Program

Magister Ilmu Hukum UNDIP

Prof. Dr. H. Barda Nawawi Arief, S.H.

KATA PENGANTAR

Syukur alhamdulillah penulis panjatkan kepada Allah, karena atas berkat dan rahmat serta karunia-Nya, penulis dapat menyelesaikan tugas akhir berupa penulisan tesis sebagai pemenuhan kewajiban dalam menempuh pendidikan di Program Pascasarjana Magister Ilmu Hukum UNDIP Kajian Sistem Peradilan Pidana. Untuk menyelesaikan tugas akhir itu, penulis sengaja mengambil materi penelitian yang berangkat dari sebuah harapan, kegalauan dan keprihatinan yang mendalam mengenai masa depan hukum khususnya ilmu hukum pidana dalam menghadapi perkembangan teknologi informasi yang cepat berubah.

Dalam penulisan tesis ini penulis memberi judul ***Hacking Sebagai Fenomena Cybercrime (Kajian Kriminologis Terhadap Fenomena Hacker Di Cyberspace)***. Penulis menyadari walaupun fakta-fakta mengenai *cybercrime* tidak dapat digambarkan secara menyeluruh dalam penulisan tesis ini, akan tetapi penulis berkeyakinan bahwa langkah sekecil apapun harus dilakukan untuk memperbaiki keadaan atau setidak-tidaknya membuka wacana baru tentang hukum dan perkembangan teknologi informasi.

Tesis ini tidak mungkin terwujud tanpa adanya bantuan dari berbagai pihak. Untuk itu pada kesempatan ini penulis ingin mengungkapkan ucapan terima kasih yang mendalam kepada :

1. **Prof. Dr Barda Nawawi Arief, S.H.,** selaku Ketua Program Pascasarjana Magister Ilmu Hukum UNDIP sekaligus sebagai Penguji Tesis ini.
2. **Bapak Prof. Dr I.S. Susanto, S.H.,** selaku pembimbing tesis yang dengan kebijaksanaan, kesabaran dan ketelitiannya telah memberikan bimbingan, arahan dan nasehat-nasehat kepada penulis serta dorongan motivasi untuk selalu menambah pengetahuan, khususnya pengembangan materi tesis di kemudian hari.

3. Bapak **Budiharto, S.H., M.S.**, selaku sekretaris Program Pascasarjana Magister Ilmu Hukum UNDIP yang telah berkenan memberikan surat pengantar untuk mengadakan penelitian di berbagai tempat.
4. **Bapak Prof. Dr Man Suparman**, selaku Dekan FH Universitas Padjadjaran dan Bapak **Dr. Ahmad Ramli, S.H.**, serta Bapak **Sigid Suseno, S.H., M.Hum**, selaku Tim Perumus RUU Teknologi Informasi FH Unpad Bandung yang telah memberikan data-data yang penulis butuhkan baik data tertulis maupun data tidak tertulis berupa pendapat maupun pandangan-pandangannya mengenai aspek hukum perkembangan teknologi informasi.
5. Bapak **Dr Ir. Budi Rahardjo,** dari Pusat Antar Universitas Bidang Mikroelektronika (PAU Mikroelektronika) ITB, Mas **Basuki, Afan Basalamah dan Adnan Basalamah**, dari Computer Network Research Group (CNRG) PAU Mikroelektronika ITB Bandung atas kesediaannya memberikan informasi yang berharga mengenai aspek teknis dari *hacking* khususnya dan cara kerja internet pada umumnya.
6. Bapak **Onno W. Purbo**, selaku pakar internet, meskipun beliau tidak mau mengajarkan teknik-teknik *hacking* kepada penulis tetapi penulis sangat menghargai jawaban-jawaban yang diberikan atas pertanyaan yang penulis ajukan lewat *e-mail*.
7. Bapak **Freddy Harris, S.H., M.Si** dan Bapak **Edmon Makarim, S.H**. dari Lembaga Kajian Hukum Ekonomi dan Teknologi Fakultas Hukum Universitas Indonesia (LKHT FH UI) atas kesediaannya menerima penulis dan sebuah wawancara yang cukup menarik terutama mengenai *cyberspace* dan *cyberlaw* serta kemungkinan pengembangan di masa yang akan datang;
8. Kepala Pusat Komputer Universitas Jenderal Soedirman beserta stafnya atas segala pelayanan yang diberikan kepada penulis terutama terhadap diskon 50% biaya penggunaan internet untuk waktu yang tidak terlalu lama, tetapi itu sudah cukup membantu. Semoga terus meningkatkan pelayanannya kepada konsumen terutama mahasiswa yang melakukan penelitian.

9. Bapak Brigjen Pol. Didi Widayadi, Kadisnfolahta Mabes POLRI, Ibu **Ir. Nunuk Mahastuti,** selaku Kepala Bagian Tata Usaha Pusat Data dan Informasi Departemen Perindustrian dan Perdagangan beserta stafnya, Bapak **Hadi Munadi** dari Biro Komunikasi PT. BEJ dan beberapa Staf Departemen Luar Negeri Bagian Pengolahan Data dan Informasi, yang telah mengijinkan dan memberikan data-data yang penulis butuhkan berkaitan dengan aktivitas internet departemen dalam melakukan pelayanan publik.
10. **Sdr. Mesnan Silalahi, MSc,** dari Sekretariat Riset Unggulan Terpadu Lembaga Ilmu Pengetahuan Indonesia (RUT LIPI) dan Bapak **Drs. Wasi Tri Prasetya,** selaku staf di Pusat Dokumentasi dan Informasi Ilmuah (LIPI) atas segala percakapannya mengenai pengelolaan dan penyajian data-data RUT/PDII LIPI melalui internet dan sebuah percakapan menarik mengenai aktivitas *hacking* yang dilakukan *cracker* yang sempat menjebol situs yang dikelolanya.
11. Bapak **Viktor** dari LPK Pratama Mulya/Indo Komputer yang selalu setia dan menyempatkan waktu di sela-sela kesibukannya memberikan bimbingan dan arahan mengenai teknik-teknik komputasi dan operasionalisasi internet.
12. Bapak **Sarwat Sarwowijoyo** (alm) dan Ibu **Samiyem** (alm), kedua orang tua penulis, yang telah melahirkan, membesarkan dan mengajarkan kebijaksanaan hidup, serta saudara-saudara yang telah mengiringi dan dengan setia membimbing, memberi arahan, nasehat serta berbagai petuah yang penulis tak terlupakan dan dapat dijadikan sebagai sumber motivasi.
13. **Rini Fidiyani, S.H., M.Hum**, isteri tersayang yang tiada henti-hentinya memberikan kasihnya serta dorongan, nasehat dan pertimbangan-pertimbangan yang bermanfaat dalam menempuh pendidikan di Program Pascasarjana Magister Ilmu Hukum Undip umumnya dan khususnya dalam penulisan tugas akhir ini.
14. Bapak **Suhaimi** dan Ibu **Isti Faiyah**, yang telah memberikan dukungan moril dan dukungan lain kepada penulis untuk menyelesaikan tugas akhir dan

terutama penulis meminta maaf apabila selama penulisan tesis ini biaya pulsa telepon membengkak akibat penggunaan internet untuk surfing penulis.

15. **Sdr. Anton Freddy Susanto, S.H., dan Bapak Sudirman Sitepu** selaku teman diskusi mengenai berbagai topik baik dalam ruang kuliah maupun dalam perjalanan ke kampus serta segala hal yang berkaitan dengan perkuliahan dan penulisan tugas akhir.

Penulis berharap apa yang ditulis dalam laporan penelitian ini dapat bermanfaat bagi kita semua secara nyata. Jikapun ada kekurangan, mohonlah ditambahkan sebab demikian sifat ilmu pengetahuan, selalu kehausan seperti lautan, meskipun tiap hari ia selalu minum dari sungai-sungai yang mengalir ke arahnya..

Semarang, Juli 2001

Penulis

Agus Raharjo

Di dunia ini tidak ada yang semulia pengetahuan,

tidak juga filsafat kehidupan

(Kata Khrisna kepada Arjuna dalam Bhagawadgita)

Penulis persembahkan kepada:

- Bapak dan Ibu tercinta
- Isteriku terkasih
- Buah hati yang belum terlahir

SUMMARY

Information technology develops in high speed due to the support of communication and computer technology. Branches of science such as chemistry, physics, biology and mathematics are the basic of such development. Internet is the backbone of information technology which has developed since 1960s as the US counter against its cold war with the Soviet Union. At the beginning internet was used for military, educational and research purposes. Since the invention of World Wide Web which consist of Hypertext Mark Up Language (HTML) documents in 1991, internet begins to be used in various field such as politics, economy, social sciences and culture.

Internet has opened a new horizon for human being because it go beyond interstate border and speed up the spread of information and the exchange of sciences and ideas among the scientist, expert, businessmen and consumers, politician and its supporters. Internet present us new space or world which is called cyberspace. Cyberspace is a our place when we are sailing in the interactive global information named internet. Internet with cyberspace offers us many kinds of hope, pleasure, easiness and adventure such as teleshoping, teleconference, teledildonic, virtual café, virtual architecture, virtual museum, cybersex, cyberparty and cyberorgasm.

Internet, besides offering hope and easiness, also arouse fears because internet also offers us the dark side which enables criminals to appear in this global interactive world. We can, among others, name computer criminals, organized crime figures, drug cartels, international money lounderers, hackers and cyberpunks, child pornography and child abduction rings, software piracy, theft of cable services, theft of telephone services, computerized stalking, terrorist rings, narcotics dealing, as well as other forms of criminal activities including plain theft, fraudelent traders and pedophiles.

One form of cyberspace crime or cybercrime is hacking which is committed by crackers. Hacking can be categorized as crime because it brings harms both to the public and private interest and is also against the public morality. Since internet can be used for multi purpose, especially politic and businesses, the social construct against hacking is also based on the interest of whose who are involved in the field of business and politics.

In Indonesia, there is no exact data about the number of those who have become victims of hacking. The victims usually do not have reliable security system so that it is easy for crackers to penetrate them. Efforts to counter hacking are done in two ways: prevention and recovery. Preventive measure is done by installing reliable and tight security system. While recovery measure is in the form of repairing the sites of website which have been the victims of hacking. This is done through various techniques.

So fat there has not been any legal protection provided by the government to the victims of hacking in particular and sites and websites owner in general. This is due to two reason, first the government does not have rule which specifically deals with cybercrime (hacking) and second the police does not have the ability to prevent and counter cybercrime. As an effort to protect website owner in the future, the government is creating a cyberlaw is expected to prevent and counter cybercrime.

RINGKASAN

Teknologi informasi berkembang sangat pesat berkat dukungan dari teknologi komunikasi dan teknologi komputer. Kimia, fisika, biologi dan matematika mendasari semua perkembangan itu. Internet merupakan tulang punggung dari teknologi informasi yang telah berkembang sejak tahun 1960-an sebagai antisipasi Amerika Serikat dalam menghadapi perang dingin dengan Uni Sovyet. Pada mulanya internet digunakan untuk kepentingan militer, pendidikan dan penelitian. Sejak diketemukannya World Wide Web yang terdiri dari dokumen-dokumen Hypertext Mark up Language (HTML) pada 1991, internet mulai digunakan untuk berbagai hal, seperti politik, ekonomi, sosial dan budaya.

Internet telah membuka cakrawala baru dalam kehidupan manusia yang menjanjikan menembus batas-batas antar negara dan mempercepat penyebaran informasi dan pertukaran ilmu dan gagasan di kalangan ilmuwan dan cendekiawan, pengusaha dan konsumen, politisi dan para pendukungnya. Internet menghadirkan kepada kita ruang atau dunia baru yang dinamakan *cyberspace*. *Cyberspace* merupakan tempat kita berada ketika mengarungi dunia informasi global interaktif yang bernama internet. Internet dengan *cyberspace*-nya menawarkan kepada manusia berbagai harapan, kesenangan, kemudahan dan pengembaraan seperti *teleshoping, teleconference, teledildonic, virtual café, virtual architecture, virtual museum, cybersex, cyberparty* dan *cyberorgasm*.

Internet, selain menawarkan harapan dan kemudahan, juga menimbulkan kecemasan-kecemasan karena internet juga menghadirkan sisi gelap yang memungkinkan para penjahat hadir di dunia informasi global interaktif ini. Sisi gelap yang hadir antara lain *computer criminals, organized crime figures, drug cartels, international money lounderers, hackers and cyberpunks, child pornography and child abduction rings, software piracy, theft of cable services, theft of telephone services, computerized stalking, terrorist rings, narcotics dealing, as well as other forms of criminal activities including plain theft, fraudelent traders, pedophiles.*

Salah satu bentuk kejahaan di *cyberspace* atau *cybercrime* adalah *hacking* yang dilakukan oleh *cracker*. *Hacking* dapat dikategorikan sebagai kejahatan karena aksinya bertentangan dengan atau merugikan kepentingan umum dan privat serta bertentangan dengan moral masyarakat. Mengingat internet digunakan untuk berbagai hal, terutama politik dan bisnis, maka konstruksi sosial kejahatan terhadap *hacking* juga didasarkan pada kepentingan-kepentingan dari para pelaku politik dan bisnis.

Di Indonesia dapat dijumpai korban-korban *hacking* yang jumlahnya tidak dapat dipastikan. Para korban umumnya tidak mempunyai sistem keamanan yang baik sehingga mudah ditembus oleh *cracker* dari luar. Upaya untuk mengantisipasi serangan *cracker* dilakukan melalui dua cara, yaitu *preventif* dan *recovery*. Upaya *preventif* dilakukan dengan memasang sistem keamanan yang baik atau ketat dan upaya *recovery* berupa pemulihan terhadap situs atau website yang telah menjadi korban *hacker* dengan berbagai teknik yang ada.

Perlindungan hukum yang diberikan oleh pemerintah terhadap korban *hacking* khususnya dan pemilik situs atau website pada umumnya sampai sekarang tidak ada, yang disebabkan karena dua hal, pertama undang-undang yang secara khusus mengatur mengenai *cybercrime* (*hacking*) belum ada dan aparat yang ada (polisi) sampai saat ini belum mempunyai kemampuan yang memadai untuk dapat melakukan pencegahan dan penanggulangan *cybercrime*. Sebagai upaya dalam rangka melindungi pemilik website di masa mendatang, sampai saat ini pemerintah sedang membuat *cyberlaw* yang diharapkan dapat mencegah dan menanggulangi *cybercrime*.

DAFTAR ISI

DAFTAR BAGAN

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Teknologi informasi (*information technology*) memegang peran yang penting baik di masa kini maupun masa yang akan datang. Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia. Hal inilah yang mendorong pertemuan Konferensi Tingkat Tinggi (KTT) negara-negara yang tergabung dalam kelompok G 8 di Okinawa, Jepang (22 Juli 2000) untuk menjadikan teknologi informasi sebagai fokus pembicaraan penting. Harapan yang digantungkan terhadap teknologi informasi oleh negara-negara maju (dan juga negara berkembang) dapat dikatakan luar biasa, karena teknologi informasi dianggap mampu memacu permintaan dan menghela kereta ekonomi dunia sehingga lebih maju dan dinamis.

Setidaknya ada dua hal yang membuat teknologi informasi dianggap begitu penitng dalam memacu pertumbuhan ekonomi dunia. Pertama, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu sendiri, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya. Kedua adalah memudahkan transaksi bisnis terutama bisnis keuangan, di samping bisnis-bisnis umum lainnya.[1]

---

[1] Kompas, 23 Juli 2000, hal. 3 dengan judul *Dari Pertemuan G8 Okinawa, Teknologi Informasi, yang Melaju dan yang Tergilas.*

Harapan yang digantungkan pada teknologi informasi begitu tinggi dan harapan itu dapat saja terwujud asal informasi itu sendiri sebagai produk dipandang baik oleh negara maju maupun negara berkembang sebagai sumber pokok pengetahuan, termasuk pengembangan keilmuan dan peradaban itu sendiri. Jika informasi dipandang dengan pandangan demikian, maka kualitas manusia akan meningkat sehingga lebih bermoral, terpelajar, terdidik dan lebih berperadaban.

Teknologi informasi oleh negara-negara yang tergabung dalam kelompok G 8, dipandang sebagai hal yang amat vital dalam petumbuhan ekonomi dunia ke depan, perluasan kesempatan belajar serta perolehan informasi masyarakat di dunia. Salah satu pasal dari **Deklarasi Okinawa** tentang masyarakat informasi global menyatakan "*Kegagalan negara-negara berkembang dalam mengikuti akselerasi teknologi informasi akan membuat mereka tidak mempunayi kesempatan berpartisipasi penuh di dalam masyarakat informasi dan masyarakat ekonomi dunia*". Memang dapat diakui bahwa kesenjangan antara negara kaya (maju) dan negara miskin (miskin sekali atau negara berkembang) dalam bidang teknologi informasi sangat lebar jaraknya.[2]

---

[2] Kompas, 23 Juli 2000, hal. 1dengan judul *Janji KTT G8 untuk Negara Berkembang, Teknologi Informasi dan Penanggulangan Infeksi*. Sebelum Deklarasi Okinawa tersebut sebenarnya hal tersebut pernah disinggung oleh **Bill Gates** dalam sebuah seminar *World Economic Forum (WEF)* di Davos, Swiss, pada akhir Januari 2000. Ia menyatakan bahwa dalam beberapa tahun mendatang kesenjangan negara kaya dan negara miskin yang sudah lebar akan semakin lebar lagi akibat perkembangan internet. Hal ini diperkuat dengan adanya survei dari *Pricewaterhouse Cooper (PwC)* bahwa 50% pimpinan perusahaan terkemuka berpendapat kesenjangan negara kaya dan miskin akan semakin lebar. Untuk memperkecil kesenjangan itu itu menurut menurut **Case** (aalah seorang pimpinan *American Online/AOL*) diperlukan lompatan teknologi agar negara miskin secara *instant* langsung memasuki era internet sehingga negara-negara berkembang di Asia sehingga tidak tertinggal dari apa yang disebut sebagai ***Revolusi Teknologi Informasi***. Lihat lebih jelas pada Republika, 17 Februari 2000, hal. 7 dengan judul *Booming Portal, Menggembirakan Sekaligus Mengkhawatirkan*

Kemajuan teknologi informasi sekarang dan kemungkinannya di masa yang akan datang tidak lepas dari dorongan yang dilakukan oleh perkembangan teknologi komunikasi dan teknologi komputer, sedangkan teknologi komputer dan telekomunikasi didorong oleh teknologi mikro elektronika, material dan perangkat lunak. Kimia, fisika, biologi dan matematika mendasari ini semua.[3]

Indonesia sebagai negara berkembang memang terlambat dalam mengikuti perkembangan teknologi informasi.[4] Hal ini tidak lepas dari strategi pengembangan teknologi yang tidak tepat karena mengabaikan riset sains dan teknologi. Akibatnya transfer teknologi dari negara industri maju tidak diikuti dengan penguasaan teknologi itu sendiri yang mengantarkan Indonesia kepada negara yang tidak mempunyai basis teknologi atau seperti apa yang dikatakan oleh **Muhammad Nur** sebagai negara industri baru semu.[5]

---

[3] Samaun Samadikun, *Pengaruh Perpaduan Teknologi Komputer, Telekomunikasi dan Informasi*, Kompas, 28 Juni 2000, hal. 52. Bandingkan dengan pendapat Dimitri Mahayana dalam *IT Applications in Convergence Age*, Makalah pada Seminar Nasional RUU Teknologi Informasi (cyberlaw) dengan tema Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi, diselenggarakan oleh Ditjen Postel, Departemen Perhubungan dan FH UNDIP Semarang, 26 Juli 2001, hal. 3. Pentingnya sains dasar bagi pengembangan internet terlihat dari contoh riset dalam bidang fisika zat padat yang didasari sepenuhnya oleh fisika kuantum menghasilkan sains dan teknologi semikonduktor, lalu diikuti oleh aplikasi pada teknologi dan industri informasi dan komunikasi. Rentetan aplikasi sains dan teknologi semikonduktor tadi menimbulkan perubahan-perubahan yang sangat penting dalam bidang ekonomi dan sosial. Aplikasi-aplikasi tersebut telah mengarahkan umat manusia pada ekonomi informasi dan mengubah secara mendasar kondisi-kondisi kerja dan struktur pekerjaan, A. King, 1995, *Science and Technologi, In Science and Power*, seperti dikutip oleh Muhammad Nur, *Beberapga Gagasan Untuk Kemajuan Teknologi Menuju Pada Kemandirian Sains*, Pidato Dies Natalis ke 41 UNDIP Semarang, 15 Oktober 1998, hal. 4.

[4] Hal ini terbukti berdasarkan survai yang dilakukan oleh ITU (*International Telecomunication Union*) terhadap 40 negara (yang dimuat pada tahun 1997) dalam pengembangan infrastruktur informasi, Indonesia menduduki urutan terakhir dari keseluruhan negara kecuali India. Tidak hanya itu, Indonesia juga berada di belakang semua negara yang menjadi pembandingnya dalam pemasokan layanan dan produk teknologi informasi, khusunya di pasar yang berkembang pesat di wilayahnya, *Dilema Pengembangan Infrastruktur Informasi Indonesia*, dalam Majalah Info Komputer Volume XII No. 8 Agustus 1998, hal. 34

[5] Muhammad Nur, *ibid*, hal. 5-6. Bandingkan dengan Jepang, Korea, Taiwan, Cina, Thailand, Malaysia dan Filipina yang menempatkan industri elektronika sebagai tulang punggung strategi industrialisasi untuk pembangunan bangsa mereka. Indonesia sebaiknya memanfaat-kan peluang yang terbuka bagi penyediaan peralatan elektronika yang sedang meledak kebutuhannya. Samaun Samadikun, *op.cit.*

Perpaduan teknologi komunikasi dan komputer melahirkan internet yang menjadi tulang punggung teknologi informasi.[6] Perkembangan internet dipicu oleh peluncuran pesawat *Sputnik* milik Uni Sovyet yang ditanggapi oleh Amerika Serikat dengan membikin proyek peluncuran pesawat luar angkasa dan pengembangan internet pada tahun 1960-an. Pada awal perkembangannya, internet digunakan atau mengabdi kepada kepentingan kekuasaan khususnya kepentingan militer Amerika Serikat.

Perkembangan teknologi umumnya dan internet pada khususnya tidak bisa dinikmati oleh orang-orang biasa seperti sekarang ini, tetapi bermain dalam tingkat elit. Pengabdian total dunia teknologi terhadap kekuasaan negara adalah inovasi perangkat perang sehingga muncul dari setiap akumulasi kekuasaan kaum bermodal melalui negara adalah perang. Penaklukan antarnegara bukan sekedar memperluas wilayah untuk kepentingan kaum feodal, tetapi penguasaan sumber-sumber bagi mesin industri. Kolonialisme berkembang dari rahim kapitalisme yang mengabaikan kemanusiaan.[7]

---

[6] Perkembangan internet sendiri tidak bisa dilepaskan dari perkembangan komputer (*hardware*) yang dimulai pada tahun 1945-1960 yang menghasilkan komputer raksasa karena ukurannya yang super besar hingga ditemukannya konsep *personal computer* pada tahun 1977 oleh **Steve Woznick** dan **Steve Jobs** dari *Silicon Valley* yang memungkinkan satu orang memegang satu komputer. Perkenbangan bidang hardware ini diikuti dengan bidang *software* komputer yang mendukung pengembangan jaringan komputer, khususnya *browser*. Sampai saat ini kurang lebih ada lima *browser* yang siap dipakai, tetapi yang sering dipakai di samping sebagai *pioneer* dan juga karena kasusnya adalah *browser* milik ***Netscape*** dan ***Internet Explorer*** dari Microsoft. Mengenai persaingan antara Netscape dengan Internet Explorer dengan seluk beluknya dapat dibaca dibaca pada tulisan Andrey Andoko, *Bill Gates Tokoh yang Dipuji dan Dimaki*, Kompas, 28 Juni 2000, hal. 76

[7] Hal ini bukan merupakan kecenderungan umum dari teknologi komunikasi. Lewat internet diharapkan informasi peradaban manusia dapat terpelihara melalui jaringan komputer di mana saja yang terintegrasi dalam sistem yang saling mendukung. Setiap kali kemunculan teknologi komunikasi baru mengubah konfigurasi masyarakat yang tadinya bersifat elitis menjadi lebih terbuka dan populis. Lihat lebih jelas pada Ashadi Siregar, *Membaca Surat Kabar Digital, Membaca Wajah Populis Teknologi Media,* Kompas, 28 Juni 2000, hal. 70.

Seusai perang dingin, internet tidak lagi digunakan untuk kepentingan militer, tetapi beralih fungsi menjadi sebuah media yang mampu membawa perubahan dalam kehidupan manusia. Internet tidak lagi hanya digunakan oleh kalangan militer, pemerintah dan ilmuwan, tetapi juga digunakan oleh pelaku bisnis, politikus, sastrawan, budayawan, musikus bahkan para penjahat dan teroris. Internet mulai digunakan sebagai alat propaganda politik,[8] transaksi bisnis atau perdagangan,[9] sarana pendidikan, kesehatan, manufaktur, perancangan, pemerintahan,[10] pronografi dan kejahatan lain.

Kehadiran internet telah membuka cakrawala baru dalam kehidupan manusia. Internet merupakan sebuah ruang informasi dan komunikasi yang menjanjikan menembus batas-batas antarnegara dan mempercepat penyebaran dan pertukaran ilmu dan gagasan di kalangan ilmuwan dan cendekiawan di seluruh dunia. Internet membawa kita kepada ruang atau dunia baru yang tercipta yang dinamakan ***Cyberspace.***

Cyberspace merupakan tempat kita berada ketika kita mengarungi dunia informasi global inter aktif yang bernama internet.[11] Istilah ini pertama

---

[8] Ingat kasus Ramos Horta yang menggunakan internet sebagai media perjuangan untuk kemerdekaan Timor Timur, terutama setelah jajak pendapat Agustus 1999, dimana Ramos Horta dengan pasukan digitalnya telah menyerang situr-situs milik Pemerintah Indonesia. Republika, 22 Agustus dan 26 September 1999, hal. 15. Dalam kaitan dengan bidang politik ini, *cracker* juga mengobrak-abrik persiapan pemilu Rumania. Mereka sukses membobol website pemantau hasil suara milik Ion Illescu (calon presiden) dan memindahkannya ke wbsite FBI. Akibatnya perkembangan dukungan calon presiden lenyap, yang muncul justru daftar nama buronan kelas kakap FBI. Jawa Pos, 1 Oktober 2000, hal, 1 dan 15.

[9] Dalam hal ini Microsoft menawarkan konsep *The Business Internet* untuk memaksimalkan manfaat internet dalam bisnis yang menjanjikan. *The Business Internet* adalah realisasi visi *Digital Nervous System* atau Sistem Syaraf Digital yang memungkinkan informasi mengalir dengan cepat dalam organisasi bisnis untuk menghadapi era ekonomi digital dan merespon peluang bisnis yang ada atau ditawarkan. Kompas, 1 Desember 1999, hal. 19

[10] Samaun Samadikun, *op.cit.*

[11] Armehdi Mahzar dalam kata pengantar buku Jeff Zaleski, *Spiritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*, Mizan, Bandung, 1999, hal. 9

kali digunakan oleh **William Gibson** dalam novel fiksi ilmiahnya yang berjudul *Neuromancer*.[12] **Bruce Sterling** memberikan definisi yang dapat memperjelas pengertian *cyberspace* ini.

> *Cyberspace* is the "place" where a telephone conversation appears to occur. Not your desk. Not inside the other person's phone, in some other city. The place between the phone. The indefinite place out there, where the two of you, two human beings, actually meet and communication.[13]

Cyberspace menampilkan realitas, tetapi bukan realitas yang nyata sebagaimana bisa kita lihat melainkan realitas virtual (*virtual reality*), dunia maya, dunia yang tanpa batas. Inilah sebenarnya dimaksud dengan *borderless world*, karena memang dalam *cyberspace* tidak mengenal batas negara, hilangnya batas dimensi ruang, waktu dan tempat[14] sehingga penghuni-penghuninya bisa berhubungan dengan siapa saja dan di mana saja sebagaimana dikatakan oleh **Bruce Sterling** lebih lanjut

> Although it is not exactly "real", "*cyberspace*" is a genuine place. Things happen there that have very genuine consequences. This "place" is not "real" but it is serious, it is earnest. Tens of thousands of people have dedicated their lives to it, the public service of public communication by wire and electronic.[15]

Cyberspace menawarkan manusia untuk "hidup" dalam dunia alternatif. Sebuah dunia yang dapat mengambil alih dan menggantikan realitas

---

[12] Memang istilah ini pertama kali dipakai oleh William Gibson, tetapi dalam konteks internet, John Perry Barlow mengkalim sebagai pengguna pertama. Penjelasan lebih lengkap dapat dibaca dalam percakapan antara John Perry Barlow dengan Jeff Zaleski, *ibid*, hal. 53

[13] Bruce Sterling, *The Hacker Crackdown, Law and Disorder on the Electronic Frontier*, Massmarket Paperback, 1990, electronic version available at http://www.lysator.liu.se/etexts/*hacker*/

[14] Onno W. Purbo, *Perkembangan Teknologi Informasi dan Internet di Indonesia*, Kompas, 28 Juni 2000, hal. 50. Penggunaan istilah borderless world dalam konteks ini berbeda dengan apa yang dimaksud oleh Kenichi Ohmae, karena dalam konteks ini istilah borderless world menunjuk kepada pergerakan dunia informasi melalui internet (yang di dalamnya dapat saja terdapat unsur ekonomi).

[15] Bruce Sterling, *op.cit.*

yang ada, yang lebih menyenangkan dari kesenangan yang ada, yang lebih fantastis dari fantasi yang ada, yang lebih menggairahkan dari kegairahan yang ada. Jagat raya *cyberspace* telah membawa masyarakat dalam berbagai sisi realitas baru yang tidak pernah dibayangkan sebelumnya, yang penuh dengan harapan, kesenangan, kemudahan dan pengembaraan seperti *teleshoping, teleconference, teledildonic, virtual café, virtual architecture, vitual museum, cybersex, cyberparty dan cyberorgasm.*[16]

Proses *cybernation* yang menimbulkan harapan akan kemudahan, kesenangan dan kesempatan itu ternyata tidak selamanya demikian karena dalam *cyberspace* juga terdapat sisi gelap yang perlu kita perhatikan sebagaimana yang dikatakan oleh **Neill Barrett**

> The internet, however, also has a darker side - in particular, it is widely considered to provide access almost exclusively to pornography. A recent, well-publicized survey suggested that over 80 % of the picture on the Internet were pornographic. While the survey result itself was found to be entirely erroneous, the observation that the Internet can and does contain illicit, objectionable or downright illegal material is perfectly valid. As we shall see, the Internet support fraudulent traders, terrorist information exchanges, pedophiles, software pirates, computer *hacker*s and many more.[17]

Senada dengan apa yang dikemukakan oleh **Neill Barrett, Mark D. Rasch** juga mengungkapkan sisi gelap dari *cyberspace* ini dengan kata-kata

> However, along the information superhighway are information superhighwaymen. .They do not shout the electronic equivalent of "stand and deliver". Rather, computer criminals, organized crime figures, drug cartels, international money lounderers, *hacker*s and "cyberpunks" are all roaming the Internet -- seeking money, information or simply an opportunity to wreak havoc and destruction. ... Computer and computer bulletin boards have been used to facilitate child pornography and child abduction rings, software piracy, theft of

---

[16] Yasraf Amir Piliang dalam pengantar buku Mark Slouka, *Ruang yang Hilang, Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan*, Mizan, Bandung, 1999, hal. 14-15.

[17] Neill Barrett, *Digital Crime, Policing the Cybernation*, Kogan Page Ltd, London, 1997, hal. 21

> cable services, theft of telephone services, computerized stalking, terrorist rings, narcotics dealing, as well as other forms of criminal activities including plain theft.[18]

Dari sekian banyak sisi gelap yang ada dalam *cyberspace*, yang menjadi fokus perhatian dalam penelitian ini adalah perbuatan yang dilakukan oleh *cracker* atau *hacker hitam*. Fenomena *cracker* dalam tahun-tahun terakhir ini memang mencemaskan karena mereka telah menggunakan keahliannya untuk melakukan kejahatan. Apa yang dilakukan *cracker* menurut **Onno W. Purbo** sangat menganggu hak asasi manusia untuk memperoleh informasi, berkomunikasi dan hak untuk berpartisipasi dalam masyarakat informasi global tanpa dibatasi dimensi fisik, ruang, waktu dan institusi. Hukum perlu mengantisipasi hilangnya batas dimensi ruang, waktu dan tempat agar internet betul-betul bermanfaat.[19]

Kecemasan terhadap aktivitas *cracker* atau *cybercrime* telah menjadi perhatian dunia, terbukti dengan dijadikannya masalah *cybercrime* sebagai salah satu topik bahasan pada Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offender* ke 8 tahun 1990 di Havana, Kuba dan Kongres ke 10 di Wina. Pada Kongres ke 8 PBB memandang perlu dilakukan usaha-usaha penanggulangan kejahatan yang berkaitan dengan komputer (computer related crime), sedangkan pada Kongres ke 10 di Wina, *cybercrime* dijadikan sebagai topik bahasan tersendiri dengan judul *crimes related to computer network*.

---

[18] Mark D. Rasch, *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, pada bab ke sebelas yang berjudul *Criminal Law and The Internet*, Computer Law Association, 1996, http://cla.org/RuhBook/chp11.htm

[19] Onno W. Purbo, *op.cit.* Bandingkan dengan Pasal 14 UU No. 39 Tahun 1999 tentang Hak Asasi Manusia

Tidak semua negara di dunia ini memberikan perhatian yang lebih besar tentang masalah *cybercrime* dan memiliki peraturannya (kecuali negara-negara maju dan beberapa negara berkembang)[20] Hal ini disebabkan oleh tingkat kemajuan dan perhatian dari hukum terhadap teknologi seperti disinyalir oleh Kongres PBB di Wina dengan ungkapan sebagai berikut :

> Reason for the lack of attention to cybercrime may include relatively low levels of participation in international electronic communications, low levels of law enforcement experience and low estimations of the damage to society expected to occur from electronic crimes.

Seperti yang telah disebutkan di atas dan jika dibandingkan dengan negara-negara maju dan beberapa negara berkembang lainnya, Indonesia termasuk negara yang lambat dalam mengikuti perkembangan teknologi informasi. Hal ini nampak dari penglihatan Bank Dunia, di mana Indonesia dipandang belum memiliki regulasi pengembangan aplikasi informatik generasi baru, terutama yang paling kritis dalam kaitannya dengan perlindungan hak cipta untuk *software, data* dan *integrated circuit*,[21] dan *cybercrime.* Kelambatan ini membawa dampak ketika terjadi *cybercrime* maka perangkat hukum yang mengatur *cybercrime* tidak ada dan penegak hukumnya pun menjadi bingung karena tidak ada pegangan untuk menindak.

Untuk memahami lebih dalam mengenai hal tersebut khususnya persoalan *cybercrime,* maka perlu dilakukan eksplorasi mengenai segi teknis dari

---

[20] Amerika Serikat telah mempunyai perangkat hukumnya dengan adanya Computer Fraud and Abuse Act 1984 yang beberapa kali telah dilakukan amandemen, di antaranya tahun 1986, 1988, 1989, 1990, 1994 dan 1996. Untuk lebih jelas mengenai perkembangan peraturan tersebut baca tulisan Robert Scalione, *Crime in the Internet: Can the Law Keep Up With a New Generation of Cyberspace Hackers,* Computer and Law Homepage, Fall 1996, http://wings.buffalo.edu/CompLaw/CompLawPapers/scalion.html. Inggris, Singapura, Malaysia, India juga telah mempunyai perangkat hukum yang mengatur mengenai kegiatan di cyberspace ini.

[21] Info Komputer, volume XII No. 8 Agustus 1998, hal. 35

aktivitas *hacker* ini yang nantinya dipadukan dengan aspek yuridis agar tercipta sinkronisasi dan harmonisasi dalam pelaksanaan atau penegakan hukum saiber atau *cyberlaw enforcement.*

B. Perumusan Permasalahan

Permasalahan *cybercrime* patut mendapat perhatian mengingat kegunaan dan harapan yang digantungkan pada internet. Untuk lebih mengetahui, mendalami dan memahami aspek teknis dan yuridis dari aktivitas *hacker*, maka dalam penelitian ini diajukan beberapa permasalahan, yaitu :

1. Seberapa jauh tahap-tahap hacking yang dilakukan oleh *hacker* dalam upaya masuk dan merusak situs atau website milik pihak lain dikonstruksikan sebagai kejahatan?
2. Bagaimanakah reaksi dan aksi para pemilik situs atau website yang menjadi korban aktivitas *hacker* tersebut?
3. Bentuk perlindungan hukum yang seperti apakah yang diberikan oleh pemerintah kepada pemilik situs atau website dari ancaman serangan *hacker*?

C. Kerangka Pemikiran

Kemajuan teknologi informasi telah mengubah pandangan manusia tentang berbagai kegiatan yang selama ini hanya dimonopoli oleh aktivitas yang bersifat fisik belaka. Lahirnya internet merubah paradigma komunikasi manusia dalam bergaul, berbisnis dan juga berasmara. Internet mengubah konsep jarak dan waktu secara drastis sehingga seolah-olah dunia menjadi kecil dan tak berbatas. Setiap orang bisa berhubungan, berbicara dan berbisnis dengan orang lain yang berada ribuan kilometer dari tempat di mana ia berada hanya dengan menekan tuts-tuts keyboard dan mouse komputer yang ada di hadapannya.

Dari segi penulisannya, internet memiliki dua arti, yaitu[22] :

1. internet

   Jaringan internet (huruf "i" kecil sebagai huruf awal) adalah merupakan suatu jaringan komputer yang mana komputer-komputer terhubung dapat berkomunikasi walaupun perangkat keras dan perangkat lunaknya berlainan (seringkali disebut juga *internetworking*)

2. Internet

   Jaringan Internet (huruf "I" besar sebagai huruf awal) adalah jaringan dari sekumpulan jaringan (*networks of networks*) yang terdiri dari jutaan komputer yang dapat berkomunikasi satu sama lain dengan menggunakan suatu aturan komunikasi jaringan komputer (*protokol*) yang sama. Protokol yang digunakan tersebut adalah TCP/IP (*Transmission Control Protocol/Internet Protocol*).

The Federal Networking Council (FNC) memberikan definisi mengenai internet dalam resolusinya tanggal 24 Oktober 1995. Definisi yang diberikan adalah sebagai berikut :

> Internet refers to the global information system that --
> (i) is logically linked together by a globally unique address space based in the Internet Protocol (IP) or its subsequent extensions/follow-ons;
> (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extension/follow-ons, and/or other IP-compatible protocols; and
> (iii) Providers, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

---

[22] Fransisca Haryanti Chandra, *Internet: Information Superhighway*, Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah VI di Semarang, 4 - 8 September 1995, hal. 1-2

Dalam membicarakan tentang jaringan komputer yang bernama internet ini, menurut Kongres PBB ke 10 di Wina ada tiga hal yang esensial pada sistem komputer dan keamanan data, yaitu *assurance confidentially, integrity or availability of data* dan *processing function*. Dalam kaitannya dengan keamanan (*security*) dan integritas (*integrity*) jaringan internet yang berbasis komputer maka tingkat keamanan yang rendah akan mengakibatkan sistem informasi yang ada tidak mampu menghasilkan unjuk kerja (*performance*) yang tinggi. Dengan kata lain keamanan dan integritas penting dalam upaya menjaga konsistensi unjuk kerja dari sistem atau jaringan internet yang bersangkutan.[23]

Dewan Eropa bekerjasama dengan Organisasi Kerjasama Ekonomi dan Pembangunan pada tahun 1985 merekomendasikan bahwa ada bahaya yang dapat menyerang ketiga hal yang esensial yang telah disebutkan dalam Kongres PBB ke 10 di Wina tersebut di atas. Rekomendasi tersebut menyebutkan ada lima serangan terhadap sistem komputer, yaitu[24] :

a. Unauthorized access, meaning access without rights to a computer system or network by infringing security measures
b. Damage to computer data or computer programs, meaning the erasure, corruption, deterioration or suppression of computer data or computer programs without rights.
c. Computer sabotage, meaning the input, alteration, erasure or suppression of computer data or computer programs, or interference with computer system, with intent to hinder functioning of a computer or telecommunication system.

---

[23] Rudi Hendarman, *Computer Fraud*, Majalah Pro Justitia UNPAR, Tahun XIII No. 2 April 1995, hal 100.

[24] Dokumen A/CONF.187/10 Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, *Crimes related to computer networks*, hal. 5. Bandingkan dengan Rudi Hendarman yang berpendapat bahwa hanya ada dua hal yang penting dalam sistem computer, yaitu keamanan (*security*) dan integritas (*integrity*),op.cit, hal. 100, sedangkan Ronny R. Nitibaskara berpendapat bahwa masalah yang paling mendesak adalah masalah keamanan, dalam *Problem Yuridis Cybercrime*, Makalah pada Seminar Sehari Cyberlaw 2000, Bandung, 29 Juli 2000, lihat juga Kompas, 29 Juli 2000. Pendapat senada diungkapkan oleh Onno W. Purba dan Tony Wiharjito dalam buku *Keamanan Jaringan Internet*, Elex Media Komputindo, Jakarta, 2000.

d. Unauthorized interception, meaning the interception, made without authorization and by technical means, of communications to, form and within a computer system or network.
e. Computer espionage, meaning the acquisition disclosure, transfer or use of a commercial secret without authorization or legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an illegal advantage for themselves or a third person.

Sistem keamanan jaringan komputer atau sistem informasi yang berbasis komputer yang terhubung ke internet perlu dilindungi dan dijaga kemutakhirannya karena keamanan jaringan internet yang sifatnya publik dan global pada dasarnya tidak aman, sehingga perlindungan sistem keamanan internet harus direncanakan dan dipahami dengan baik agar dapat melindungi investasi dan sumberdaya di dalam jaringan komputer tersebut secara efektif.[25]

Internet atau jaringan komputer yang besar sesungguhnya tidak menganggu manusia, malahan membantu manusia dalam mencapai tujuan-tujuan yang bersifat positif, seperti dalam bidang bisnis ada *e-commerce* atau *e-trade*, sebagai media pendidikan politik dan sebagainya. Faktor manusia yang menggunakan internet dengan tujuan jahat yang membuat pemakai internet tidak nyaman. Manusia inilah yang dalam dunia *cyberspace* dinamakan *hacker hitam/cracker*.

Hacker secara harafiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup atau melakukan perusakan melalui komputer.[26] *Hacker* dapat juga didefinisikan sebagai orang-orang yang gemar

---

[25] Onno W. Purbo & Tony Wiharjito, *op.cit.* hal. 1-2. Perusahaan yang mengandalkan teknologi informasi semakin lama semakin banyak, seiring dengan hal tersebut korban teknologi informasi juga bertambah secara signifikan, mulai dari virus komputer, pencurian data, sampai perusakan perangkat keras. Untuk lebih jelas lihat Laporan Utama pada Majalah Info Komputer, volume XI No. 5 Mei 1995, hal. 36-48

[26] Republika, 22 Agustus 1999, hal. 15

mempelajari seluk beluk sistem komputer dan bereksperimen dengannya.[27] Penggunaan istilah *hacker* terus berkembang seiring dengan perkembangan internet, tetapi terjadi pembiasan makna kata. *Hacker* yang masih menjunjung tinggi atau memiliki motivasi yang sama dengan perintis mereka, *hacker-hacker* MIT disebut *hacker* topi putih (*White hat hackers*). Mereka masih memegang prinsip bahwa menghack adalah untuk tujuan meningkatkan keamanan jaringan internet. *Hacker* dalam pengertian yang kedua adalah mereka yang dengan kemampuan yang dimiliki melakukan kejahatan baik pencurian nomor kartu kredit sampai perusakan situs atau website milik orang lain. *Hacker* ini selalu berperang dengan *hacker* topi putih yang menyebut mereka dengan istilah *cracker* (*hacker* hitam). Akibat publikasi dari aksi-aksi *hacker* dari kedua kelompok tersebut di atas maka muncullah kelompok *hacker* yang melakukan aksinya secara terang-terangan dan cenderung menyombongkan diri apabila berhasil melakukan penyusupan atau perusakan. *Hacker* demikian dinamakan *Vandal Komputer* atau *Bogus Hacker*.[28]

Hacking yang dilakukan oleh *hacker* hitam pada intinya adalah *unauthorized access* sebagai *first crime*. Setelah *hacker* dapat masuk ke jaringan internet pihak lain maka *hacker* dapat melakukan kejahatan lain seperti *damage to data or computer espionage* atau dapat juga mengirimkan virus pada e-mail orang lain yang akan menyebar apabila e-mail itu dibuka.

Serangan *cracker* memang luar biasa, bahkan Kementrian Pertahanan Amerika Serikat yang bermarkas di Pentagon mencatat jaringan komputer

---

[27] Gede Artha Azriadi Prana, *Hacker, Sisi Lain Legenda Komputer*, Adigna, Jakarta, 1999, hal. 22
[28] *Ibid*, hal, 35-39

mereka setiap hari menjadi sasaran 100 *hacker*. "*Ketergantungan kita terhadap komputer menyebabkan kita terus menerus mudah diserang, semua itu mudah diserang jika terjadi perang informasi atau jika jadi sasaran hacker atau teroris saiber*", kata **Richard Clark**, Koordinator Infrastruktur Proteksi dan Counter Teroris pada *National Security Council.* Teroris, sikap bermusuhan terhadap negara, kriminal, *hacker*, mereka semua menjelma menjadi tantangan, menciptakan tekanan baru dari musuh bagi intelejen, staf pertahanan dan penegak hukum di seluruh dunia. Dalam dua tahun terakhir, FBI mencatat kejahatan yang dilakukan meningkat dua kali lipat, bahkan sampai Oktober 1999 tercatat sebanyak 800 kasus yang harus ditangani FBI.[29]

Perkembangan *hacker* dalam dua tahun terakhir ini juga sangat pesat. Menurut *President Internet Security Advisory's Group*, **Ira Winkler**, kelompok *hacker* yang dinamakan *ankle biters* atau *bogus hackers* yang nampaknya cuma main-main saja, sehingga mudah diamankan jika sistem administrasi saja yang diserangnya. Mereka biasanya cukup senang jika sudah dapat membuat repot mesin printer yang akan digunakan.[30]

Penghuni *cyberspace* sebenarnya bukan hanya *hacker*, tetapi sebagai dunia yang telah lama ada terutama jika kita menyimak definisi yang diungkapkan oleh **Bruce Sterling**. Termasuk di dalamnya adalah *telephone technicians, engineers, operators* dan *researchers.*[31] Selain *hacker* mereka yang disebut belakangan adalah para veteran karana keberadaannya jauh lebih dahulu

---

[29] Republika, 6 Januari 2000, hal. 15

[30] *Ibid.*

[31] Menurut sejarahnya, *cyberspace* ada pertama kali ketika Alexander Graham Bell menemukan telepon pata 1876. Mereka yang disebut sebagai veteran adalah para perintis atau yang pertama

ada dibandingkan dengan *hacker*.[32] Perkembangan internetlah yang membuat *hacker* lebih populer dibandingkan dengan para penghuni *cyberspace* lainnya.

Aktivitas *cracker* yang makin lama makin mencemaskan ini tentunya menimbulkan keragu-raguan pada manfaat internet yang telah ditawarkan. Berjuta-juta keuntungan yang diharapkan tentunya akan lenyap jika cracker dapat masuk dan merusak investasi yang telah ditanamkan pada pengembangan internet sebagai sarana aktivitas manusia. Untuk itu aktivitas cracker ini perlu di kriminalisasikan. Tetapi sebelum sampai pada tahap itu maka perlu terlebih dahulu dilakukan pengkajian dari segi kriminologi yang hasinya dapat dipakai sebagai bahan pertimbangan dalam proses kriminalisasi aktivitas *hacker* tersebut.

Untuk memahami realitas sosial ataupun realitas virtual dari aktivitas *hacker* yang ada, bentuk pemahaman terhadap aspek hukum saja tidaklah cukup untuk menjelaskan secara mendasar realitas yang melingkupi *cybercrime* ini. Oleh karena itu dalam menjelaskan persoalan ini secara lebih mendalam diperlukan bentuk pemahaman dan pandangan baru yang melibatkan ilmu-ilmu sosial lainnya.

Phillip Nonet dan **Philip Selznick** mengemukakan bahwa ilmu hukum selalau memiliki keterkaitan yang luas dengan berbagai disiplin ilmu. Konsep abstrak tentang kewajiban hukum berbicara tentang perbedaan pemahaman

---

menjadi penduduk *cyberspace*, sedangkan *hacker* baru ada pada dekade 1960-an ketika pertama kali dikembangkan internet. Bruce Sterling, *op.cit.*

[32] Aktivitas para veteran ini di *cyberspace* sering diganggu oleh penghuni *cyberspace* lain yang bersifat illegal dengan cara mencuri pulsa atau memperlambat jalanya pulsa telepon yang pelakunya disebut dengan nama *phreaker*.

tentang bagaimana hukum itu bekerja dan digunakan.[33] Untuk sampai pada tahap pemahaman itu, ilmu hukum saja tidak cukup karena hukum itu sendiri dalam bekerjanya dipengaruhi oleh beberapa faktor seperti faktor sosial, budaya, ekonomi, politik dan sebagainya. Dengan berbekal pengetahuan hukum dan pengetahuan sosial lain maka dapat digunakan untuk mendiagnosa kesulitan-kesulitan yang dihadapi dan menimpa hukum.

Solusi yang dilontarkan oleh **Nonet** dan **Selznick** untuk membuat ilmu hukum lebih hidup dan relevan adalah dengan melakukan reintegrasi antara hukum, politik dan berbagai teori dalam ilmu sosial lainnya. Dalam tahap ini kita memperhatikan masalah-masalah hukum ditinjau dari sudut pandang ilmu pengetahuan sosial. Kemudian untuk memahaminya kita mengajukan kerangka kerja dengan membandingkan masing-masing penalaran tersebut (penalaran dari bidang hukum dan bidang sosial yang diintegrasikan) untuk melakukan analisis terhadap permasalahan yang ada.[34]

Perkembangan kajian kriminologi sebenarnya tidak bisa dilepaskan dengan keberadaan hukum pidana dan sosiologi hukum itu sendiri. Seiring perjalanan kriminologi, hukum pidana dan sosiologi hukum memiliki lahan kajian yang saling berkaitan sehingga tidak mengherankan apabila denan memfungsikan keberadaan ketiga kajian itu secara komprehensif dan integral akan memperoleh pemahaman yang jauh lebih baik dan mendekati kebutuhan senyatanya dari realitas yang ada.[35]

---

[33] Phillip Nonet dan Philip Selznick, *Law and Society in Transition, Toward Responsive Law*, Harper and Row, New York, 1978, hal. 1

[34] *Ibid*, hal. 3-4

[35] Mulyana W. Kusuma, *Realitas Sosial Kejahatan*, Prisma, LP3ES, Jakarta, 5 Mei 1982, hal. 39

Kajian kriminologi dalam hal ini menggunakan kriminologi kritis karena dengan menggunakan kriminologi kritis akan memperoleh penjelasan yang lebih lengkap, lebih baik dan lebih luas jika dibandingkan dengan pengkajian yang dilakukan oleh kriminologi klasik maupun positif. Kriminologi kritis dapat mengungkap proses-proses bagaimana terjadinya kejahatan *saiber/cybercrime*, tidak hanya secara teknis, tetapi juga segi lain yang relevan seperti psikologi, etika, moral dan sebagainya.

Kriminologi kritis tidak akan menerima realitas sosial kejahatan saiber yang dilakukan *cracker* di *cyberspace* begitu saja (*taken for granted*), artinya tidak secara tergesa-gesa menyatakan bahwa apa yang dilakukan oleh *cracker* sebagai suatu kejahatan atau perilaku menyimpang. Fenomena yang terjadi harus dipahami secara obyektif dan kritis, dan bukan merupakan sesuatu yang jatuh dari langit. Untuk sampai pada tahap ini memerlukan proses yang tidak singkat.

Teori kriminologi yang akan membantu dalam menjelaskan fenomena *hacker* di *cyberspace* adalah teori realitas sosial kejahatan dari **Richard Quinney** dan teori *Labeling* dari **Howard Becker**. **Richard Quinney** dalam teorinya menjelaskan bahwa realitas sosial adalah hasil dari konstruksi sosial. Dalam penjelasan teori ini, **Quinney** menulis:

> "A theory that help us begin to examine the social reality of crime. Applying this theory, we think of crimes as it is affected by that's dynamics that's molded the society's social, economic and political structure. We recognize how criminal fits into capitalist society. The legal orders give reality to the crime problem. Everything that's make up crime's social reality, including the application of criminal law, behavior patterns of those who are defines as criminal, and the construction of an ideology of crime, is related to the established legal

> order. The social reality of crime is constructed on conflict in our society.[36]

Realitas sosial yang bermacam-macam ternyata tidak nampak sebagai realitas yang sebenarnya ketika realitas itu tidak dipahami secara benar dan kritis. Realitas sosial tidak hanya sekedar menjelaskan suatu fenomena, tetapi lebih jauh juga menafsirkan suatu situasi atau keadaan sebagaimana dikatakan oleh **Mulyana W. Kusuma**:

> Pemahaman kita mengenai realitas tidaklah semata-mata merupakan suatu koleksi lepas dari pengertian yang tidak saling berhubungan yang menunjuk pada kejadian-kejadian dan objek-objek dalam lingkungan kita, melainkan merupakan hirarki yang secara sistematik ter-organisasikan melalui mana kita memahami dan menafsirkan dunia.[37]

Mengenai persoalan pemikiran atau pemahaman kritis terhadap realitas sosial, **I.S. Susanto** memberikan penjelasan sebagai berikut :

> Realitas sosial dapat diartikan sebagai kenyataan tentang kejadian-kejadian dan sebagai gambaran tentang kenyataan atau pengetahuan tenang kenyataan. Yang pertama menggambarkan tentang kejadian-kejadian dalam masyarakat yang dapat dilihat, didengar dan dibaca dalam kehidupan sehari-hari yang dipandang sebagai realitas tentang fenomena, sedangkan yang kedua merupakan gambaran atau pengetahuan yang kita miliki tentang kenyataan sosial atau disebut juga sebagai realitas konseptual. Pembicaraan tentang realitas sosial karenanya lebih mengarah pada pengertian realitas konseptual, sebab peranannya sangat penting dalam kehidupan sosial.[38]

Realitas dari aktivitas *cracker* selalu dikonseptualisasikan sebagai sebuah realitas yang menyimpang dan hal tersebut mengakibatkan ruang gerak *hacker* topi putih menjadi lebih sempit. Konseptualisasi ini berakibat *cracker* dari semua golongan dikonotasikan sebagai orang yang memiliki perilaku

---

[36] Richard Quinney, *Criminology: Analysis and Critique of Crime in America*, Brown and Co, New York, 1975, hal. 37

[37] Mulyana W. Kusuma, *Aneka Permasalahan Dalam Ruang Lingkup Kriminologi*, Alumni, Bandung, 1981, hal. 19

[38] I.S. Susanto, *Pemahaman Kritis Terhadap Realitas Sosial*, Makalah pada Lokakarya Nasional untuk Pengembangan Sumber Daya IMKA di Karangpandan, 12-17 Agustus 1992, hal. 1

menyimpang dan perbuatannya dikategorikan sebagai kejahatan. Bentuk pemahaman yang lebih tajam terhadap realitas sosial kejahatan atau perilaku yang menyimpang menurut **Richard Quinney** dapat dilakukan dengan melakukan pemahaman kritis terhadap hukum (*legal order*) maupun pendekatan kritis terhadap kejahatan dalam bidang kriminologi.[39]

Perhatian terakhir kriminologi tentang tindakan kriminal modern adalah apa yang paling banyak mendapat perhatian. Dalam hal ini apa yang menjadi masalah kejahatan dapat memberitahukan kita tentang masyarakat di mana kita tinggal, maka untuk mengatasi kasus atau tindakan kriminal itu kita harus tahu masyarakat yang bersangkutan sehinga tahu mana yang harus diprioritaskan.[40] Dalam pemikiran kriminologi juga telah tumbuh perspektif, di mana kriminologi yang ada sekarang tumbuh dari cara pandang yag dilandasi oleh meningkatnya kesadaran tentang sifat politis dan teknis dari kejahatan.

Kriminologi kritis memandang fenomena kejahatan sebagai konstruksi sosial, oleh karena itu kriminologi kritis mempelajari tentang proses-proses di mana kumpulan tertentu dari orang-orang dan tindakan-tindakan ditujukan sebagai kriminal pada waktu dan tempat tertentu. Kriminologi kritis tidak hanya mempelajari perilaku dari orang-orang yang didefinisikan sebagai penjahat tetapi juga perilaku dari agen-agen kontrol sosial (aparat penegak hukum), di samping mempertanyakan mengapa tindakan tersebut dikatakan sebagai kejahatan. Dengan demikian untuk memahami kejahatan, perlu diperlajari seluruh proses kriminaliasi, dalam arti baik proses-proses yang mempengaruhi pembentukan

---

[39] Richard Quinney, *op.cit.*, hal. 9

[40] John Hagan, *Studying Criminology: Why Criminology*? Dalam Modern Criminology, Crime, Criminal Behaviour and Its Control, diterjemahkan oleh Mufid menjadi *Mengenal Kriminologi* dalam Majalah Legality, Vol. 3/II/Maret-Agustus 1994, hal. 47

undang-undang yakni dijadikannya perbuatan tertentu sebagai tindak pidana maupun dalam bekerjanya hukum.[41]

Munculnya teori Labeling merupakan akibat dari berkembangnya pemikiran kritis pada tahun 1960-an. Teori Labeling seperti yang dikemukakan oleh **Howard S. Becker** dalam bukunya *Outsiders*, menyatakan bahwa kejahatan sebagai hal yang problematik dan merupakan hasil dari batasan masyarakat, sebab ukuran-ukuran atau norma-norma yang dilanggar tidak bersifat universal dan tidak dapat dirubah. Ada dua dalil yang dikemukakan dalam teorinya itu, yaitu pertama kelompok sosiallah yang menciptakan penyimpangan dengan membuat peraturan, bahwa barang siapa melanggarnya akan menghasilkan penyimpangan dan kedua perilaku menyimpang adalah perilaku yang oleh orang-orang diberi cap demikian.[42]

Kehadiran internet telah membawa pergeseran pada penilaian tentang kehidupan. Pengguna atau pemakai internet yang menjadi masyarakat internet atau *netizen* mempunyai kehidupan ganda, sebagai mahluk yang ada di dunia nyata dan mahluk yang ada dalam dunia maya. Kedua posisi tersebut secara fleksibel bisa berubah sesuai dengan keinginan aktor, termasuk di dalamnya adalah perubahan dari orang baik-baik di dunia nyata menjadi penjahat kelas berat di dunia maya atau sebaliknya. Bahasa yang digunakan mereka dalam berinteraksi dan beraksi pun bisa berbeda. Kebiasaan menggunakan simbol dalam berkomunikasi melalui media internet adalah hal yang biasa dan *netizen* juga saling memahami hal ini.

---

41 I.S. Susanto, *Kejahatan Korporasi*, BP. UNDIP Semarang, 1995, hal. 8-9

42 Howard S. Becker, *Outsiders: Studies in the Sociology of Deviance*, The Free Press, New York, hal. 9. Lihat juga I.S. Susanto, Diktat Kriminologi, FH UNDIP Semarang, 1985, hal. 76

Untuk membahas persoalan tersebut, maka dipergunakan teori-teori yang terdapat dalam paradigma definisi sosial, khususnya teori interaksionisme simbolik. Dalam paradigam definisi sosial, manusia adalah merupakan aktor yang kreatif dari realitas sosialnya. Realitas sosial bukan merupakan alat yang statis daripada paksaan fakta sosial, artinya tindakan manusia tidak sepenuhnya ditentukan oleh norma-norma, kebiasaan-kebiasaan, nilai-nilai dan sebagainya yang kesemuanya itu tercakup dalam konsep fakta sosial.[43]

Interaksionisme simbolik menurut **George Herbert Mead** mempelajari tindakan sosial dengan mempergunakan teknik instrospeksi untuk dapat mengetahui barang sesuatu yang melatarbelakangi tindakan sosial itu dari sudut aktor. Sedangkan **Herbert Blumer** berpendapat bahwa interaksionisme simbolik menunjuk kepada sifat khas dari interaksi antara manusia. Kekhasannya adalah bahwa manusia saling menerjemahkan dan saling mendefinisikan tindakannya. Bukan sekedar reaksi belaka, tetapi reaksi yang sudah melalui proses interpretasi oleh si aktor.[44] Inilah jalinan yang erat antara teori interaksionisme simbolik dengan teori kritis dalam kriminologi yang memperhatikan aspek-aspek dari tindakan atau perbuatan seseorang terhadap stimulus yang diterima.

Ide bahwa kenyataan atau realitas sosial muncul melalui proses interaksi sangat penting dalam teori interaksi simbol. Dalam karya **Mead**, teori ini meliputi analisa mengenai kemampuan manusia untuk menciptakan dan

---

[43] George Ritzer, *Sosiologi Ilmu Pengetahuan Berparadigma Ganda*, Rajawali, Jakarta, 1985, hal. 50

[44] *Ibid*, hal. 60-61. Pemberian reaksi terhadap stimulus yang diterima diberikan melalui proses-proses yang tercipta karena manusia mempunyai kepribadian dan pengetahuan sendiri yang tercipta selama proses kehidupan dan karena manusia mepunyai kemampuan untuk menciptakan sasaran tindakan-tindakannya sendiri.

memanipulasi simbol-simbol. Pada proses interaksi atau komunikasi antar individu atau kelompok terdapat sisi yang tidak kelihatan. Dalam pandangan **Mead** dikatakan bahwa hubungan antara komunikasi dengan kesadaran subjektif sedemikian dekatnya sehingga proses berpikir subjektif atau refleksi dapat dilihat sebagai sisi yang tidak kelihatan (*covert*) dari komunikasi itu. Tentu ada segi-segi pengalaman subjektif individual yang tidak dapat sepenuhnya dibagikan kepada orang lain.[45]

Perspektif interaksionisme simbol mengenai penyimpangan memulai dengan suatu pengakuan bahwa penyimpangan tidak hanya sekedar suatu manifestasi suatu ciri pembawaan sejak lahir atau cacat kepribadian. Sebaliknya penyimpangan itu dihasilkan sebagai akibat dari suatu tipe proses interaksi tertentu. Identitas mereka yang menyimpang serta subkulturnya muncul dari proses interaksi karena mereka yang menyimpang itu secara bertahap mengambil dan menyesuaikan diri dengan identitas-identitas penyimpangan seperti yang dicapkan kepada mereka oleh wakil-wakil masyarakat. Inilah dasar bagi teori cap (*labeling theory*) di mana masyarakat sendiri menciptakan orang-orang yang menyimpang dengan membuat peraturan yang pelanggarannya menimbulkan penyimpangan dan memperlakukan secara khusus beberapa dari mereka yang bersalah dalam pelangaran seperti itu. Dari hal tersebut di atas terlihat bahwa penggunaan teori kriminologi dan teori sosiologi saling berkaitan atau saling melengkapi satu sama lain.[46]

Penelitian ini menggunakan metode kriminologi dan sosiologi. Ini bukan tanpa alasan karena seperti yang dikatakan oleh **Ian Taylor, Paul Walton**

---

[45] Doyle Paul Johnson, *Teori Sosiologi, Klasik dan Modern* (terjemahan Robert M.Z. Lawang), Gramedia, Jakarta, 1990, hal. 4, 12-13

[46] *Ibid*, hal. 40 - 41

dan **Jack Young** yang mengutip pendapat **Edwin M. Schur** tentang pendekatan sosiologi dan kriminologi terhadap kejahatan, perilaku menyimpang di masyarakat dan permasalahan sosial mengemukakan bahwa pendekatan yang dilakukan oleh sosiologi dan kriminologi terhadap kejahatan, perilaku menyimpang dan permasalahan sosial adalah jauh lebih luas dan lebih tajam apabila dibandingkan dengan melakukan pendekatan yang hanya terpaku pada pendekatan legalistik positivistis.[47]

Hasil dari kajian kriminologi dapat dijadikan sebagai bahan untuk melakukan kriminalisasi.[48] Kriminalisasi, dekriminalisasi dan depenalisasi merupakan istilah yang terkait satu sama lain. Dalam hal ini **Sudarto** berpendapat

> Kriminalisasi dimaksudkan proses penetapan suatu perbuatan orang sebagai perbuatan yang dipidana, proses ini diakhiri dengan terbentuknya undang-undangm di mana perbuatan itu diancam dengan suatu sanksi yang berupa pidana. Dekriminalisasi mengandung arti suatu proses di mana dihilangkan sama sekali sifat dapat dipidananya sesuatu perbuatan. Dekriminalisasi harus dibedakan dengan depenalisasi yang berarti perbuatan yang semula diancam pidana, ancaman pidana itu dihilangkan akan tetapi masih dimungkinkan adanya penuntutan dengan cara lain yaitu melalui hukum pidana atau hukum administrasi.[49]

Persoalan kriminalisasi dan dekriminalisasi sebagaimana telah diajukan dalam simposium pembahasan hukum pidana nasional di Semarang tahun 1980, harus dilakukan dengan pendekatan yang berorientasi kepada kebijakan sosial. Dalam simposium tersebut dikemukakan bahwa masalah kriminalisasi dan

---

[47] Ian Taylor, Paul Walton, Jack Young, *The Criminology for a Social Theory of Deviance, International Library of Sociology*, edited by John Rex, Routledge and Kegan Paul, London & Boston, 1973, hal. 140.

[48] Sudarto mengatakan bahwa kriminologi bukan ilmu yang melakukan kebijakan, kriminologi adalah disiplin yang *non policy making*, akan tetapi hasil penemuannya dapat digunakan untuk melaksanakan kebijakan. Yang melaksanakan kebijakan adalah unsur-unsur pelaksana politik kriminal. Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1977, hal. 161

[49] *Ibid*, hal. 37-38

dekriminalisasi atas suatu perbuatan haruslah sesuai dengan politik kriminal yang dianut oleh bangsa Indonesia.[50] Mengenai permasalahan kriminalisasi, dekriminalisasi dan penalisasi ini, **I.S. Susanto** berpendapat bahwa dalam kaitannya dengan ketiga proses tersebut, maka kerangka kajian kritis dalam kriminologi telah melakukan sebuah upaya untuk memahami secara kritis tentang proses-proses pembentukan undang-undang dan sekaligus berkerjanya.[51]

Penelitian ini akan berusaha mengungkap realitas aktivitas *hacker* di *cyberspace* dengan panduan kerangka teori kriminologi kritis seperti teori tentang realitas sosial kejahatan, teori labeling dan teori sosiologis seperti teori fakta sosial dan teori simbolik interaksionisme. Teori-teori ini tidak dijadikan sebagai dasar kerja (*basic work*) akan tetapi sebagai pendahuluan untuk memasuki lapangan kualitatif.

D. Tujuan Penelitian

Penelitian terhadap aktivitas *hacker* berupa hacking di *cyberspace* ini bertujuan untuk :

1. Menganalisa dan mengklasifikasikan tahap-tahap hacking yang dilakukan oleh *hacker* dalam upaya masuk dan merusak situs atau website milik pihak lain dikonstruksikan sebagai kejahatan.
2. Menganlisis dan mengevaluasi reaksi dan aksi para pemilik situs atau website yang menjadi korban aktivitas *hacker* tersebut.
3. Mengetahui dan memahami perlindungan hukum yang diberikan oleh pemerintah kepada pemilik situs atau website dari ancaman serangan *hacker*.

---

[50] Barda Nawawi Arief, *Kebijakan Legislatif dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, BP UNDIP Semarang, 1996, hal. 36

[51] I.S. Susanto, *loc.cit.*, hal. 13 dan 24

E. Kontribusi Penelitian

Penelitian tentang *cybercrime* pada dasarnya merupakan penelitian kriminologi.[52] Namun dari penelitian ini diharapkan dapat memberikan sumbangan atau menyempurnakan sistem peradilan di Indonesia.[53] Untuk itu penelitian ini diharapkan dapat memberikan kontribusi berupa :

1. Kontribusi Teoritis

Penelitian ini diharapkan dapat memberikan gambaran mengenai aktivitas *hacker* berupa hacking di *cyberspace* dikaitkan dengan teori-teori kriminologi dan sosiologi, dan memberikan sumbangan pemikiran bagi pengembangan teori hukum (khususnya hukum pidana) dan teori kriminologi di era *cyberspace*

2. Kontribusi Praktis

Penelitian ini secara praktis memberikan informasi tentang fenomena *hacker* di *cyberspace* termasuk aktivitasnya sehingga muncul konstruksi sosial bahwa perbuatan yang dilakukan *hacker* merupakan kejahatan. Bagi para pengambil kebijakan atau pembuat undang-undang termasuk penegak hukum, penelitian ini diharapkan dapat digunakan sebagai acuan atau sumbangan pemikiran untuk proses kriminalisasi aktivitas *hacker* di *cyberspace* karena hukum sekarang dituntut untuk menyesuaikan dengan kondisi dan situasi.

---

[52] Menurut Marc Ancel, Modern Criminal Science terdiri dari tiga komponen, yaitu Criminology, Criminal Law dan Penal Policy. Di kutip dari Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung, 1996, hal. 23

[53] Mardjono Reksodipuro, *Kriminologi dan Sistem Peradilan Pidana*, Lembaga Kriminologi UI, Jakarta, 1994, hal. 147. Bandingkan dengan I.S. Susanti yang berpendapat bahwa penelitian kriminologi dapat mewujudkan perbaikan dalam sistem peradilan pidana baik dalam hal penegakan hukumnya, perhatian terhadap hak terdakwa dan korban, organisasi (birokrasi) penegakan hukum dan perbaikan undang-undang itu sendiri. I.S. Susanto, op.cit. hal. 14.

Bagi para praktisi internet maupun orang-orang yang memiliki perhatian terhadap internet, penelitian ini diharapkan dapat menyumbangkan wacana pemikiran mengenai penggunaaan internet supaya tidak melakukan hacking dan terhindar dari ancaman dan perusakan situs atau website oleh *hacker*.

F. Metode Penelitian

1. Metode Pendekatan

Penelitian ini bermaksud untuk mengungkap fenomena *cybercrime* di *cyberspace*, proses bagaimana seorang *hacker hitam/cracker* malakukan kejahatan dan bagaimana bekerjanya hukum dalam penanggulangan *cybercrime* yang selama ini terjadi. Berdasarkan permasalahan yang diteliti, maka penelitian in menggunakan pendekatan hukum yang sosiologis,[54] karena peneliti menelusuri secara mendalam (*in depth*) mengenai kenyataan terhadap suatu fenomena empirik dan penerapan hukum pidana dalam konteks permasalahan yang sesuai dengan konteks sosialnya.

Penelusuran secara mendalam terhadap aktivitas *cracker* (*cybercrime*) di *cyberspace* akan membawa peneliti kepada bentuk-bentuk aktivitas *hacker*, sehingga konsep yang dihasilkan dari penelitian ini bukan hanya sekedar menggunakan dan menguji sebuah teori, namun berupaya membangun pemahaman baru yang lebih dapat menjelaskan realitas sosial yang terjadi.

---

[54] Penelitian hukum sosiologis yang dipergunakan di sini bukan berarti meniadakan aspek penelitian hukum normatif, tetapi kedua-duanya digunakan hanya metode penelitian hukum normatif tidak digunakan sebagai metode utama dalam penelitian ini. Penggunaan metode penelitian hukum normatif terutama dilakukan melalui inventarisasi hukum, penemuan hukum in abstracto dan perbandingan hukum. Ronny Hanitijo Soemitro, *Metode Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta, 1994, hal. 34-35

Dalam penelitian sosiologis, perhatian peneliti akan lebih terfokus pada upaya untuk memahami realitas sosial dari aktivitas *cracker* yang ada. Peneliti berupaya untuk memahami keadaan hukum dalam keadaan yang senyatanya, di mana dalam kenyataannya keberadaan hukum tidaklah steril tetapi dipengaruhi oleh aspek-aspek non hukum.[55]

Penelitian ini merupakan penelitian kualitatif.[56] Penggunaan metode penelitian kualitatif dimaksudkan agar peneliti dapat mengungkapkan secara lebih mendalam fenomena *cracker* di *cyberspace* karena metode kualitatif lebih mudah menyesuaikan dengan keadaan atau berhadapan dengan kenyataan ganda. Di samping itu *cyberspace* merupakan sesuatu yang keberadaannya belum lama diperhitungkan seiring dengan perkembangan internet. Pendekatan kualitatif mampu mengungkapkan makna-makna sosial yang ada dan tersembunyi di *cyberspace*.

Melihat titik fokus penelitian ini kepada bentuk pemaparan dan pemahaman mengenai sebuah fenomena yang menimbulkan sikap, perilaku dan tindakan, metode penelitian kualitatif akan lebih tepat digunakan. Hal ini dilakukan karena metode kualitatif dapat melakukan penyesuaian secara cepat dan fleksibel terhadap suatu realitas yang ada dan mampu menanggapi secara responsif terhadap perubahan-perubahan yang terjadi seketika di lapangan.[57] Di

---

55 Satjipto Rahardjo, *Hukum Itu Tidak Steril*, Suara Pembaruan, 31 Agustus 1989, hal. 2

56 Ada beberapa istilah yang artinya sama atau sejenis dengan metode penelitian kualitatif ini seperti inkuiri naturalistik atau alamiah dan sebagainya. Lebih jelas lihat Lexy J. Moleong, *Metodologi Penelitian Kualitatif*, Remaja Rosdakarya, Bandung, 1995, ha. 2-3

57 Bruce A. Chodwick et.al., *Metode Penelitian Ilmu Sosial* (terjemahan Sulistia dkk) IKIP Semarang Press, 1991, hal. 246. Bandingkan dengan Lexy J. Moleong, *op.cit* dan Sanafiah Faisal, *Penelitian Kualitatif, Dasar-dasar dan Aplikasi*, Y A 3 Malang, 1990.

samping itu hubungan yang terjalin antara peneliti dan yang diteliti lebih bersifat interaktif.

Mengingat penelitian ini adalah penelitian kriminologis, metode penelitian yang dilakukan akan lebih spesifik lagi apabila menunjuk kepada metode penelitian dalam kriminologi.[58] Metode penelitian kriminologi yang dipakai dalam penelitian ini adalah yang dikemukakan oleh **Richard Quinney**. **Richard Quinney** mengajukan empat metode dalam melakukan penelitian di bidang kriminologi, yaitu *positivistic, the cosial construction, the fenomenological and critical.* Keempat metode ini dapat digunakan untuk memahami dan membangun secara kritis teori tentang kejahatan (*develop a critical theory of crime*).[59]

Keempat metode tersebut akan digunakan karena memang saling berkaitan. Metode positivistik akan digunakan untuk mengkaji keberadaan hukum pidana dalam kaitannya dengan *cybercrime* yang dilakukan oleh *cracker*, bagaimana sikap dan tanggapan hukum pidana terhadap jenis kejahatan yang baru ini. Metode konstruksi sosial akan digunakan peneliti untuk mengungkapkan hal-hal yang diyakini bersama oleh para *netizen* (warta/masyarakat internet) sebagai sebuah ideologi di *cyberspace*, mengungkap fenomena dan latar belakang aktivitas *hacker/cracker*, aktivitas aparat keamanan

---

[58] Metode-metode tersebut antara lain metode pengobatan, statistik kejahatan, hubungan antara kejahatan dengan kondisi-kondisi menurut statistik, studi kasus, riwayat hidup, penelitian partisipan dan jangka panjang. Lebih jelas lihat pada Soedjono Dirdjosisworo, *Pengantar Penelitian Kriminologi*, Ghalia Indonesia, Jakarta, 1995, hal. 22-23. Penggunaan metode ini lebih menitikberatkan pada metode kuantitatif dan eksperimental, padahal dalam penelitian kriminologi perlu untuk memahami pengertian yang subjektif dan pemahaman yang mendasarkan pada akal sehat (*common sense*) khususnya dalam mencari jawaban tentang kosa kata baru seperti konstruksi sosial, perpektif manusia, tentang realitas fenomenologi, ethnometodology, yang bisa dilakukan dengan metode kualitatif bukan kuantitatif. I.S. Susanto, 1995, *op.cit.*, hal, 25.

[59] Richard Quinney, *op.cit.*, hal. 9

atau penegak hukum dalam menangani jenis kejahatan ini. Metode fenomenologi digunakan untuk memahami aktivitas *hacker* yang marak dalam beberapa tahun terakhir ini dan metode kritis digunakan untuk memahami secara kritis dari seluruh aspek penelitian yang ada dan mempertanyakan kembali kebenaran-kebenaran yang diyakini sebagai sebuah ideologi para *netizen* (lebih khusus lagi adalah *hacker*).

2. Lokasi Penelitian

Penelitian untuk memahami fenomena *hacker* yang berupa *cybercrime* dilakukan di kota-kota yang selama ini merupakan tempat atau lokasi pusat perkembangan internet dan korban aktivitas *hacker* di Indonesia terutama di Jakarta dan Bandung. Sedangkan untuk penelitian yang berupa penjelajahan dunia *cyberspace* akan dilakukan dengan menggunakan internet.

3. Sampel Penelitian

Sesuai dengan metode kualitatif, maka sampel penelitian tidak diambil sebagai representasi guna menarik generalisasi yang berlaku bagi populasi. Konsep sampel dalam penelitian kualitatif berkaitan dengan bagaimana memilih informan atau situasi sosial tertentu yang dapat memberikan informasi yang mantap dan terpercaya mengenai elemen-elemen yang ada (karakteristik elemen-elemen yang tercakup dalam fokus atau topik penelitian)[60]

Pemilihan sampel atau informan penelitian dilakukan secara *purposive sampling*,[61] sehingga ditentukan sampel atau informas awal dalam penelitian ini adalah :

---

60 Sanafiah Faisal, *op.cit.*, hal. 56

61 Mengenai teknik penarikan sampel ini lebih jelas dapat dilihat pada Mario SW Sumardjono, *Pedoman Pembuatan Usulan Penelitian, Sebuah Panduan Dasar*, Gramedia, Jakarta, 1996, hal. 32-32

a. Para ahli di bidang internet atau teknologi informasi baik di dalam maupun di luar negeri
b. Para pemilik atau pengelola jasa pelayanan internet (*Internet Service Provider*)
c. Pemilik atau pengelola situs atau website yang menjadi korban *hacker*
d. Para ahli hukum, sosial dan budya budaya yang berkecimpung atau memiliki perhatian terhadap *cybercrime* baik di dalam maupun di luar negeri
e. Masyarakat pengguna internet (*netizen*)

Sampel atau informasi berikutnya akan berkembang mengikuti prinsip "bola salju" (*snow ball*) dan pilihan sampel akan berakhir setelah terdapat indikasi "tidak munculnya" variasi atau informasi baru yang terkait dengan penelitian ini.[62]

4. Sumber Data

Sumber data utama dalam penelitian kualitatif adalah kata-kata dan tindakan, selebihnya adalah data tambahan seperti dokumen dan lain-lain.[63] **Heribertus Sutopo** mengatakan bahwa sumber data dalam penelitian kualitatif adalah manusia dengan tingkah lakunya, peristiwa, dokumen, arsip dan benda-benda lain.[64] Oleh karena itu dalam penelitian ini sumber data utama adalah kata-kata, tingkah laku dan peristiwa yang ada dari fenomena *hacker* di *cyberspace*.

Meskipun dikatakan bahwa sumber di luar kata-kata dan tindakan merupakan sumber tambahan atau kedua, tetapi keberadaannya tidak bisa

---

62 Sanafiah Faisal, *op.cit.*, hal. 158-159
63 Lexy J. Moleong, *op.cit.*, hal. 112
64 Heribertus Sutopo, *Pengatar Penelitian Kualitatif, Dasar-dasar Teoritis dan Praktis*, Pusat Penelitian UNS, Surakarta, 1998, hal. 23

diabaikan. Data tambahan tersebut berupa sumber tertulis yang dapat dibagi atas sumber buku dan majalah ilmiah, arsip, dokumen pribadi dan dokumen resmi. Sumber data tambahan ini dapat membantu memberikan masukan untuk menganalisis sekaligus memahami makna-makna yang ada dan tersembunyi dari kumpulan data.

5. Alat Pengumpul Data

Sesuai dengan ciri khas dari penelitian kualitatif, maka menurut **Goetz** dan **LeCompte**, strategi pengumpulan data dalam penelitian kualitatif ini dapat dikelompokkan menjadi dua cara pokok, yaitu metode interaktif dan non interaktif.[65] Metode interaktif meliputi interview dan observasi berperan, sedangkan metode non interaktif meliputi observasi tidak berperan dan *content analysis* dokumen dan arsip.

Lexy J. Moleong menegaskan bahwa alat pengumpul datanya adalah pengamatan, wawancara, catatan lapangan dan penggunaan dokumen.[66] Wawancara dilakukan secara mendalam baik formal dan informal secara berulang kali. Wawancara juga dilakukan secara terbuka dengan maksud agar subjek penelitian tahu bahwa mereka sedang diwawancarai dan tahu maksud dari wawancara tersebut.[67] Dalam hal-hal tertentu peneliti dapat menanyakan pandangan responden tentang banyak hal yang sangat bermanfaat untuk menjadi dasar bagi penelitian lebih lanjut. Dalam kedudukan ini subjek penelitian lebih berperan sebagai informan daripada sekedar responden.[68]

---

65 *Ibid*
66 Lexy J. Moleong, *op.cit.*, hal 117-160
67 *Ibid*, hal. 137
68 Heribertus Sutopo, *op.cit.*, hal. 24

Wawancara formal dilakukan terhadap informan yang memiliki jabatan atau kedudukan tertentu yang memerlukan prosedur perijinan untuk mewawancarainya, namun tidak menutup kemungkinan digunakan forum lain untuk mewawancarainya semisal forum seminar. Termasuk dalam wawancara ini adalah wawancara tertulis dengan informan yang berada di luar daerah atau luar negeri yang tidak dapat dijangkau dengan dana yang tersedia, sehingga wawancaranya akan menggunakan fasilitas e-mail. Wawancara dengan *netizen* dilakukan baik secara langsung maupun tidak langsung melalui forum *mailing list.*

Selain wawancara, keterampulan observasi juga digunakan untuk memperoleh data non verbal (misalnya ekspresi informan, penampilan fisik dan sebagainya) yang sifatnya melengkapi hasil wawancara maupun untuk mengisi hal-hal yang tak mungkin terjangkau oleh wawancara. Namun hal penting yang perlu diperhatikan adalah bahwa pendekatan awal maupun dalam proses pemerolehan data, peneliti menggunakan empati, yaitu sikap pengertian yang mendalam terhadap mereka yang terlibat kasus atau menjadi korban dari *cybercrime* namun tanpa keterlibatan emosional dan mengadili. Semua hasil yang diperoleh melalui wawancara secara mendalam, pengamatan dan *life history* akan menjadi data primer penelitian, sedangkan studi literatur bermanfaat dalam memberikan kerangka pemikiran penelitian ini.

Dalam kaitan dengan penggunaan teori simbolis interaksionisme, Blumer berpendapat bahwa metode interaksi-simbolis merupakan pengkajian fenomena sosial secara langsung. Ia mengetengahkan dua model pengamatan (inquiry) yang memungkinkan pengkajian fenomena sosial secara langsung yaitu

penjelajahan dan pemeriksaan.[69] Penjelajahan dalam penelitian ini dilakukan dengan menggunakan internet dengan masuk menjadi warga masyarakat internet atau *netizen*.

6. Metode Analisis Data

Pendekatan yang dipakai dalam penelitian ini adalah induksi konseptualisasi. Dengan pendekatan ini peneliti bertolak dari fakta atau informasi (data) untuk membangun konsep, hipotesa dan teori. Dari fakta atau informasi ini bergerak ke arah tingkat abstraksi yang lebih tinggi yang berkembang menjadi pernyataan-pernyataan tentang definisi nominal, makna teoritis atau kontent substantif dari suatu konsep.[70]

Dalam penelitian kualitatif dengan pendekatan grounded research data merupakan sumber teori. Teori yang berupa penjelasan mengenai fenomena sebenarnya diwujudkan dalam kelangsungan penyelenggaraan penelitian yaitu dengan menggalinya keluar dari dalam data yang dikumpulkan. Jadi teori ini sebenarnya tertanam dalam data. Bagan di bawah ini memperjelas pengertian di maksud.[71]

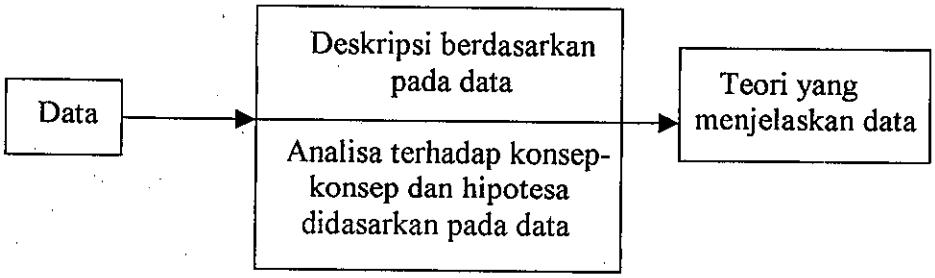
---

69 Penjelajahan (*exploration*) menurut Blumer merupakan metode fleksibel yang memberi peluang bagi peneliti "bergerak ke pemahaman yang lebih tepat mengenai bagaimana masalah seseorang harus dikemukakan, mempelajari data apa yang tepat, mengembangkan ide-ide mengenai jalur-jalur hubungan bagaimana yang signifikan dan mengembangkan peralatan konseptual seseorang dari sudut apa yang sedang dipelajarinya mengenai dunia kehidupan. Margaret M. Poloma, *Sosiologi Kontemporer*, RajaGrafindo Perkara, Jakarta, 1994, hal. 270.

70 Sanafiah Faisal, *op.cit.*, hal. 90

71 Ronny Hanitijo Soemitro, *"Grounded Research" Dalam Penelitian-penelitian Ilmu Sosial*, Majalah Masalah-masalah Hukum No. 9 Tahun 1993, hal. 32

Bagan I
Metode dan Analisis Data Dalam Penelitian Kualitatif



Dalam tahap analisis data ada tiga komponen pokok yang harus disadari sepenuhnya yaitu *data reduction, data display* dan *conclusion drawing.* Ketiga komponen ini berlaku saling mengait baik sebelum, pada waktu dan sesudah pelaksanaan pengumpulan data secara pararel yang umumnya disebut model analisis mengalir (*flow model of analysis*). Ketiga jenis kegiatan analisis dan kegiatan pengumpulan data itu sendiri merupakan proses siklus dan interaktif. Dalam model analisis interaktif ini peneliti harus siap bergerak di antara empat "sumbu" kumparan selama pengumpulan data, selanjutnya bolak-balik di antara kegiatan reduksi, penyajian dan penarikan kesimpulan atau verifikasi selama sisa waktu penelitian. Dalam pengertian ini analisis data kualitatif merupakan upaya yang berlanjut, berulang dan terus menerus. Masalah reduksi data, penyajian data dan penarikan kesimpulan atau verifikasi menjadi gambaran keberhasilan secara berurutan sebagai rangkaian kegiatan analisis yang saling susul menyusul.[72]

Untuk mempertajam fokus masalah yang diteliti, maka dipergunakan beberapa teknik analisis, yaitu analisis domain, taksonomi, komponensial dan

---

[72] Matthew B. Miles dan A. Michael Huberman, *Analisis Data Kualitatif*, UI Press, Jakarta, 1992, hal. 19-20

tema kultural.[73] Analisis domain dipergunakan pada tahap eksplorasi menyeluruh, yaitu dengan pengumpulan informasi yang sebanyak-banyaknya tentang internet dan fenomena *hacker* di *cyberspace*. Analisis taksonomi menguaraikan bagaimana hacking dilakukan oleh *hacker* dari masa ke masa sampai sekarang. Di samping itu diuraikan juga mengenai faktor-faktor yang menyebabkan hacking dikatakan sebagai kejahatan dan beberapa teori kriminologi yang membahas karakter penyimpangan dari *cybercrime*. Analisis komponensial menganalisa berbagai faktor legal dan ekstra legal yang berperan dalam menciptakan aktivitas *hacker* sebagai kejahatan dan bagaimana lembaga penegak hukum menangani kejahatan jenis ini. Analisis tema kultural merupakan upaya untuk mencari "benang merah" dari fenomena atau aktivitas yang dilakukan *hacker* di *cyberspace*. Dalam analisis ini dipergunakan beberapa teori kriminologi antara lain teori realitas sosial kejahatan, teori labeling dan teori sosiologi yaitu interaksionisme simbolik

Dari deskripsi data dan analisis data tersebut yang didasarkan pada teori kriminologi dan sosiologi kemudian dibuat abstraksi yang mengarah pada usulan konseptualisasi dan teorisasi berupa pernyataan tentang aktivitas *hacker* di *cyberspace*. Hasil penarikan abstraksi diharapkan menjadi pedoman dalam memahami hacking sebagai fenomena *cybercrime*.

G. Sistematika Penulisan

Sistematika penulisan dari tesis ini terdiri dari 4 (empat) bab. Masing-masing bab membahas materi yang saling berkaitan dengan tema sentralnya. Bab satu memuat antara lain mengenai latar belakang permasalahan, perumusan

---

[73] Sanafiah Faisal, *op.cit.*, hal. 90

permasalahan, kerangka teoritik, tujuan penelitian, kegunaan penelitian, metodologi penelitian dan sistematika penulisan.

Bab kedua berupa tinjauan pustaka yang berisi antara lain mengenai sejarah internet, fasilitas-fasilitas yang terdapat dan dapat digunakan dalam internet, cara menggunakan internet, *cyberspace* dan realitas virtual. Bab kedua ini juga dilengkapi dengan studi tentang penggunaan hasil-hasil teknologi untuk melakukan kejahatan dan pemahaman kejahatan berdasarkan perspektif krimiologi kritis yang membahas mengenai pemahaman kritis terhadap kejahatan, pendekatan interaksionis simbolik dalam kriminologi kritis dan kriminalisasi, dekriminalisasi dan depenalisasi.

Bab ketiga merupakan uraian mengenai hasil penelitian dan pembahasan atas permasalahan yang diteliti. Terdapat tiga bahasan, yaitu pertama pembahasan mengenai tahap-tahap hacking yang dikonstruksikan sebagai kejahatan. Kedua membahas mengenai reaksi dan aksi yang dilakukan oleh pemilik situs dan korban cracker/hacker hitam dan ketiga membahas tentang perlindungan hukum yang diberikan oleh pemerintah terhadap terhadap pemilik situs dari ancaman serangan hacker.

Bab keempat merupakan bab penutup yang berisi kesimpulan dan saran. Diharapkan pada bab ini dapat memberikan kesimpulan penelitian yang dapat digunakan sebagai sarana untuk mengembangkan teori kriminologi, hukum pidana dan sosiologi hukum pidana.

BAB II

TINJAUAN PUSTAKA

A. INTERNET

1. Sejarah dan Perkembangan Internet

Sejarah dan perkembangan internet tidak bisa dilepaskan dari perang dingin antara Uni Sovyet (USSR) dan Amerika Serikat yang mulai mengemuka sejak usainya Perang Dunia II. Uni Sovyet memulai perang dingin dalam bidang teknologi dengan meluncurkan *Sputnik*, satelit bumi buatan yang pertama pada tahun 1957. Sebagai respon atas stimulus yang diberikan oleh Uni Sovyet, Amerika Serikat membentuk *Advanced Research Project Agency* (ARPA) pada tahun 1958. Dibentuknya ARPA menjadikan *Department of Defense* (DoD) Amerika Serikat memimpin dalam pemanfaatan ilmu pengetahuan dan teknologi yang diterapkan untuk kepentingan militer.

Usaha yang dilakukan militer Amerika itu didasarkan pada kekhawatiran terhadap ancaman perang nuklir yang bisa saja terjadi. Untuk itu Amerika mengambil langkah dengan mengamankan atau melindungi data-data dan sistem komunikasi yang telah dibangun agar tidak dapat dihancurkan. Kekhawatiran ini terungkap dari laporan yang dibuat oleh **Paul Baran** dari Rand Corporation yang berjudul *On Distributed Communication* yang isinya adalah sebagai berikut

> Baran's research, done under a grant from the U.S. Air Force, discusses how the U.S. military could protect its communications system from

> serious attack. He outlines the principle of "redundancy of connectivity" and explores various models of forming communications system and evaluating their vulnerability.
> The report proposes a communications system there would be no obvious central command and control point, but all surviving points would be able to re-establish contact in the event of an attack on any one point. Thus damage to a part would not destroy the whole and its effect on the whole would minimized.
> One of his recommendations is for a national public utility to transport computer data, much in the way the telephone system transport voice data. "Is it time now to start thinking about a new and possibly non-existent public utility," Baran asks, " acommon user digital data communication plant designed specifically for the transmission of digital data among a large set of subscribers?"[1]

Kekhawatiran itu munculkan keinginan di kalangan militer Amerika Serikat (dibantu oleh akademisi dari berbagai universitas) untuk membuat suatu jaringan komunikasi yang dapat menghindari kehancuran data dan arsip rahasia negara lainnya. Deskripsi pertama yang tercatat dari interaksi sosial yang dapat dilakukan melalui *networks* telah ditulis dalam *series of memos* oleh **J.C.R. Licklider** dari *Massachusetts Institute of Technology* (MIT) pada Agustus 1962. Bersama **W. Clark** dia membuat paper dengan judul *On-Line Man Computer Communication* yang di dalamnya mendiskusikan tentang konsep *Galactic Networks.* **Licklider** memimpikan interkoneksi secara global melalui seperangkat komputer di mana setiap orang dapat secara cepat mengakses data dan program dari berbagai tempat. **Licklider** kemudian menjadi orang pertama yang memimpin *Computer Research Program* di *Defense Advanced Research Project Agency* (DARPA) yang dimulai pada Oktober 1962. Dia meyakinkan

---

[1] Laporan Rand Corporation oleh Paul Baran tahun 1962 sebagaimana dikutip oleh Ronda Hauben dalam *The Development of the International Computer Network From Arpanet to Usenet News (On the Nourishment or Impediment of the NET_Commonwealth).* Unpublised draft: Usenet newsgroup news.admin.misc article number 2577. Dapat juga dijumpai pada Henry Edward Hardy, *The History of the Net*, versi html, 14 Desember 1994, dapat dijumpai di http://www.ocean.ic.net/ftp/doc/nethist.html

teman-temannya seperti **Ivan Sutherland, Bob Taylor** dan peneliti MIT, **Lawrence G. Roberts** mengenai pentingnya konsep jaringan (*networking concept*).

Sebelum peristiwa tersebut di atas, pada 31 Mei 1961, **Leonard Kleinrock** dari MIT mempublikasikan papernya yang berjudul *Information Flow in Large Communication Nets*. Paper ini merupakan paper pertama tentang teori *packet-switching*.[2] **Kleinrock** meyakinkan **Roberts** bahwa ada kemungkinan secara teoritis, komunikasi menggunakan *packets* lebih baik daripada *circuit* yang telah menjadi langkah utama pengembangan jaringan komputer.

Pada tahun 1965, ARPA mensponsori studi tentang *Cooperative Network of Time-Sharing Computer* untuk mengembangkan jaringan komputer. Untuk mewujudkan hal tersebut, **Roberts** bekerjasama dengan **Thomas Merrill** menghubungkan komputer TX-2 di Massachusetts (Lincoln Lab. MIT) ke AN/FSQ-32 pada *System Development Corporation* (Santa Monica, California) dengan *dial up* saluran telepon berkecepatan rendah. Inilah tonggak pertama kali dibangunnya *wide-area network*. Sebagai hasil dari eksperimen itu telah diwujudkan dalam *time-shared computers* yang dapat berkerja bersama-sama secara baik dalam menjalankan program dan mendapatkan data yang dibutuhkan pada mesin *remote*, tetapi *telephone circuit switched system* secara total tak cukup bekerja.

---

[2] Packet switching adalah pemecahan data menjadi bagian-bagian kecil (disebut datagram) yang masing-masing dibungkus dengan informasi tambahan (alamat tujuan, alamat pengirim dan sebagainya) menjadi suatu paket. Paket ini kemudian dikirimkan melalui rute yang berbeda-beda ke suatu tujuan. Gede Artha Azriadi Prana, *Hacker, Sisi Lain Legenda Komputer*, Adigna, Jakarta, hal. 10

Sebagai kelanjutan dari usaha membentuk jaringan komputer, **Lawrence G. Roberts** meluncurkan desain pertama dari ARPANET dalam papernya *Towards a Cooperative Network of Time-Shared Computers* pada Oktober 1966. Setelah meluncurkan desainnya itu, **Roberts** pergi ke DARPA untuk mengembangkan jaringan komputer dan dengan cepat membuat rancangan untuk ARPANET yang dipublikasikan menjadi buku pada tahun 1967. Pada waktu konferensi di mana dia mempresentasikan papernya, ada juga paper tentang *packet-switching* dari Inggris yang dibuat oleh **Donald Davies** dan **Roger Scantlebury** dari *National Physical Laboratory* (NPL). **Scantlebury** menyatakan kepada **Roberts** tentang kerja NPL seperti yang **Paul Baran** dan yang lainnya kerjakan di RAND.[3]

Desain ARPANET didiskusikan oleh **Larry Roberts** pada April 1967 saat pertemuan ARPA IPTO PI di Ann Arbor, Michigan. Simposium ACM pada bulan Oktober 1967 membicarakan tentang *Operating Principles* di Gatlinburg, Tennessee dan diadakan pertemuan pertama tiga team independen *packet network* (RAND, NPL, ARPA). NPL di Middlesex, Inggris telah mengembangkan *NPL Data Network* di bawah pimpinan **Donald Watt Davies** yang telah menciptakan istilah *packet*. Jaringan NPL sendiri pada waktu itu telah mencoba *packet switching* dengan menggunakan kecepatan 768 kbps.

---

[3] RAND Corporation sendiri telah menulis paper tentang *packet switching networks for secure voice in military* pada tahun 1964 dalam bentuk proposal yang konsepnya telah diumumkan oleh Paul Baran. Pengembangan *packet switching* waktu itu dilakukan di MIT (1961-1967), RAND (1962-1965) dan NPL (1964-1967), di mana semua prosedur telah dipararelkan. Dalam pengembangan *packet switching* itu diusulkan saluran dengan kecepatan tinggi untuk digunakan pada desain ARPANET dengan menaikkan kapasitas dari 2.4 kbps (*kilo bytes per second*) menjadi 50 kbps. *Ibid*

Pada Agustus 1968, **Roberts** dan komunitas yang dibiayai oleh DARPA telah menghaluskan struktur dan spesifikasi dari ARPANET. RFQ diluncurkan oleh DARPA untuk mengembangkan salah satu komponen kunci dari *packet switches* yang dinamakan *Interface Message Processors* (IMP's). Hampir bersamaan dengan waktu tersebut, Bolt Beranek and Newman Inc. (BBN) yang dipimpin oleh **Frank Heart** memenangkan kontrak untuk membangun IMP's. Pada Oktober 1968 University of California Los Angeles (UCLA) dipercaya untuk membangun *Network Measurement Center*.

Selama tim BBN bekerja mengembangkan IMP's, **Bob Kahn** memegang peranan penting dari keseluruhan desain arsitektur ARPANET, tipologi jaringan telah didesain dan dioptimalkan oleh **Roberts** yang bekerja bersama **Howard Frank** dan timnya di *Network Analysis Corporation*, dan sistem ukuran jaringan yang disiapkan oleh tim **Kleinrock's** di UCLA. Sementara itu *Network Working Group* (NWC) yang dikepalai oleh **Steve Crocker**, mengembangkan *host level protocol* untuk komunikasi melalui ARPANET.

Sebagai hasil dari pengembangan teori *packet switching* oleh **Kleinorck's** yang difokusnya pada analisa desain dan ukuran, *Network Measurement Center* di UCLA telah diseleksi menjadi *node*[4] pertama dari ARPANET pada 2 September 1969 dan dengan demikian *host* komputer

---

[4] Ini berarti switch pertama (yang diketahui sebagai Interface Message Processor-IMP's) tiba pada akhir pekan Hari Buruh pada 1969 dan tim UCLA yang terdiri dari 40 orang dan dipmpin oleh Kleinorck telah menyediakan kemampuan untuk menghubungkan komputer pertama kali ke IMP. Leonard Kleinrock's Personal History/Biography, The Birth of the Internet, dapat dijumpai di http://www.isco.org/internet/history/birth.html. Nodes are stood up as BBN build each IMP's (Honeywell DDP-516 mini computer with 12K of memory; AT7T provides 50 kbps line. Robert Hobbes Zakon, *Hobbes' Internet Timeline v5.1*, dapat dijumpai di http://www.isco.org/guest/internet/History/HIT.html

pertama telah terhubungkan. Sistem yang dipakai di UCLA adalah *Scientific Data System Sigma 7* (SDS SIGMA 7, SEX). Perjuangan UCLA untuk dipercaya sebagai *node* pertama dari rencana ARPA membangun jaringan ini tidak bisa dilepaskan dari usaha keras tim mereka seperti dikatakan oleh **Vinton G. Cerf:**

> This is how I wound up working at the Network Measurement Center on the implementation of a set of tools for observing the behavior of the fledgling ARPANET. The team included **Stephen Crocker, Jon Postel**, who has been the RFC editor from the beginning; **Robert Braden**, who was working at the UCLA computer center, **Michael Wingfield**, who built the first interface to the Internet for the Xerox Data System Sigma 7 computer which had originally been the Scientific data System (SDS) Sigma 7, and **David Crocker**, who became one of the central figures in electronic mail standards fot the ARPANET and the Internet. **Mike Wingfield** built the BBN 1822 interface for Sigma 7, running at 400 Kbps, which pretty fast at the time.[5]

Node kedua dipasang di Stanford Research Institute (SRI) pada 1 Oktober 1969 melalui proyek **Doug Englebrecht** tentang *Augmentation of Human Intellect.* SRI didukung Network Information Center yang dipimpin oleh **Elizabeth (Jake) Feinler**, termasuk fungsi pemeliharaan nama *host* untuk pembuatan alamat seperti direktori pada RFC (*Request for Comment*) yang untuk pertama kalinya telah diluncurkan oleh **Steve Crocker** pada tanggal 7 April 1969. Satu bulan kemudian setelah SRI terhubung ke ARPANET, pesan pertama dari host ke host telah dikirim dari Laboratorium Kleinrock's ke SRI. Sistem yang dipakai SRI adalah SDS940/Genie.

Dua node bertambah di University of California Santa Barbara (UCSB) pada 1 November 1969 dan University of Utah pada Desember 1969. Dua node terakhir yang terpasang mengaplikasikan proyek visualisasi, dengan **Glen Culler**

---

[5] Vinton Cerf, sebagaimana dikatakan kepada Bernard Aboba, *How the Internet Came to Be*, dapat dijumpai di http://www.isoc.org/internet/history/vcerf.html.

dan **Burton Fried** di UC Santa Barbara mencari metode untuk men*display* penggunaan fungsi matematika (*Culler-Fried Interactive Mathematics*) dengan menggunakan sistem IBM 360/75, OS/MVT. **Robert Taylor** dan **Ivan Sutherland** dari Utah mencari metode representasi 3 (tiga) dimensi (*Graphics*) melalui net dengan menggunakan sistem DEC PDP-10, Tenex. Pada akhir 1969, 4 (empat) host komputer telah terhubung bersama-sama ke dalam ARPANET.

Pada tahun 1969 ini, University of Michigan dan Wayne State University mendirikan X.25 sebagai jaringan yang diperuntukkan bagi kalangan kampus. Peristiwa pada tahun ini yang perlu dicatat adalah bahwa penelitian mengenai *networking* meliputi dua cara kerja, yaitu kerja yang mendasari jaringan dan kerja pada bagaimana menggunakan jaringan. Tradisi ini terus berlanjut sampai sekarang.

Komputer yang terhubung ke ARPANET bertambah dengan cepat selama beberapa tahun berikutnya seiring dengan proses pekerjaan untuk melengkapi *host to host protocol* dan jaringan software lainnya. Publikasi pertama dari *host to host protocol* ARPANET dilakukan oleh **C.S. Carr, S. Crocker** dan **Vinton G. Cerf** dalam papernya yang berjudul *Host-Host Communication Protocol in the ARPA Network* di AFIPS Proceedings of SJCC pada tahun 1970. Laporan pertama tentang ARPANET di AFIPS adalah mengenai *Computer Network Development to Achieve Resource Sharing.* ALOHAnet menjadi *packet radio network* pertama yang dikembangkan oleh **Norman Abramson** dari University of Hawaii dan beroperasi pada Juli 1970 dan kemudian terhubung ke ARPANET pada tahun 1972.

ARPANET sendiri pada tahun 1972 mulai menggunakan *Network Control Protocol* (NCP) yang merupakan *host-to-host protocol* pertama yang dibuat oleh **Steve Crocker**. Dengan selesainya *host-to-host protocol* ARPANET yang dinamakan NCP itu, menjadikan ARPANET sebagai tempat yang lengkap untuk mengimplementasikan NCP selama periode 1971-1972. Pengguna jaringan akhirnya dapat memulai mengembangkan aplikasinya.

Pada mulanya kemajuan untuk memperoleh desain protokol, membangun dan menyebarkannya sangat lambat sehingga pada tahun 1971 hanya ada 19 node yang direncanakan oleh ARPANET.[6] Pada akhir 1971, **Larry Roberts** di DARPA memutuskan bahwa seseorang membutuhkan motivasi yang serius untuk mendapatkan sesuatu. Pada bulan Oktober 1972 Ketika diadakan International Conference on Computer Communication (ICCC) pada Oktober 1972 di Washington DC, **Larry** minta kepada **Bob Kahn** untuk mengatur demo publik ARPANET. **Bob Kahn** mengambil kesempatan ini dengan menyiapkan orang-orangnya.[7]

Demo publik yang pertama kali itu sendiri berjalan sukses dan menjadi kejutan bagi orang-orang di AT&T yang semula meragukan apakah demo itu

---

6 Bandingkan dengan pendapat Robert Hobbes Zakon yang mencatat pada tahun ini ada 15 node (23 hosts) yang terpasang , yaitu di UCLA, SRI, USCB, Univ. of Utah, BBN, MIT, RAND, SDC, Harvard, Lincoln Lab, Stanford, UIU(C), CWRU, CMU, NASA/Ames. Robert Hobbes Zakon, *op.cit.*

7 Sekelompok orang yang terlibat dalam demonstrasi itu kemudian menjadi legenda dalam sejarah internet, yaitu Bob Metcalfe yang bertanggung jawab untuk dokumentasi, Ken Pogran, David Clark dan Noel Chiappa yang menolong dalam pengembangan awal ring-based local area network dan gateway yang menjadi produk Proteon dan ditunjukkan dalam slide, Crocker dan Postel termasuk di sana. Jack Haverty yang kemudian menjadi kepada arsitek jaringan dari Oracle dan telah lulus dari MIT, Frank Heart yang memimpun proyek BBN, David Walden, Alex McKenzie, Severo Ornstein dan beberapa lainnya dari BBN yang mengembangkan IMP dan TIP. Vinton G. Cerf, *op.cit.*

akan berjalan dengan baik. Pada waktu konferensi, sekumpulan ahli bersidang.[8] Pada waktu itu **Vinton G. Cerf** mengemukakan pendapatnya

> I'm sure I have left out some and possibly misremembered others. There were a lot of other people, at least thirty, all of whom had come to this conference because of a serious academic or business interest in networking.

Selama berlangsungnya ICCC itu terjadi percakapan (*chat*) dari komputer ke komputer. Percakapan lewat komputer ini sebelumnya telah diujicobakan pertama di UCLA dan diulangi pada waktu konferensi berlangsung. *Chat* ini kemudian dikembangkan oleh **Jarkko Oikarinen** pada tahun 1988 menjadi *Internet Relay Chat* (IRC). Pada waktu yang sama dibentuk *International Network Working Group* (INWG). **Steve Crocker** yang sekarang di DARPA setelah meninggalkan UCLA tidak bersedia memimpin INWG dengan alasan tidak ada waktu sehingga dia mengusulkan **Vinton G. Cerf** sebagai ketuanya.[9]

Peristiwa lain yang perlu dicatat pada akhir 1971 dan tahun 1972 adalah penemuan program e-mail (*email program*) untuk mengirimkan pesan melalui jaringan distribusi oleh **Roy Tomlison** dari BBN. Program ini asalnya berasal dari dua program lainnya yaitu *an intra-machine email program*

---

[8] Orang-orang tersebut di antaranya adalah Donald Davies dari National Physical Laboratory, Inggris, Remi Despres dari Prancis, Larry Roberts dan Barry Wessler dari BBN, Gesualdo Le Moli peneliti pada Italian Network, Kjell Samuelson dari Swedish Royal Institute, John Wedlake dari British Telecom, Peter Kirstein dari Univ. College London, Louis Pouzin yang memimpin INRIA di Prancis, Roger Scantlebury dari NPL, dan Alex McKenzie dari BBN. Vinton G. Cerf, *ibid.* Kesuksesan demo ini kemudian diikuti dengan demo yang kedua yang terdiri dari tiga jaringan internet pada Juli 1977. Dalam demo itu telah dikirim *packets* yang melewati 94.000 mil perjalanan dan tidak kehilangan sebuah *bit* pun. Uraian lengkap mengenai demo tiga jaringan internet ini dapat dibaca pada Vinton Verf, as told to Bernard Aboba, *op.cit.*

[9] INWG ini melakukan identifikasi kebutuhan untuk mengkombinasikan usaha dalam penambahan teknologi jaringan. Dalam hal ini Cerf berafiliasi dengan International Federation of Information Processing (IFIP). Pada tahun 1974 INWG ini menjadi IFIP WG 6.1. Robert Hobbes Zakon, *op.cit*

(SENDMSG) dan *an experimental file transfer program* (CPYNET). Kemudian **Roy Tomlison** memodifikasi program email untuk ARPANET dan e-mail menjadi terkenal. Tanda @ dipilih sebagai tanda pada *Tomlison's Model 33 Teletype* yang berarti di/pada (*at*). **Larry Robert** tidak ketinggalan, untuk pertama kalinya ia menulis program manjemen e-mail untuk daftar, bacaan terseleksi, file, mengirimkan dan merespon dari pesan.[10] Dari sini e-mail terbuka sebagai aplikasi jaringan terbesar pada waktu itu terbukti dari penelitian yang dilakukan para peneliti di ARPA menunjukkan bahwa komposisi lalu lintas di ARPANET 75% adalah e-mail. Ini adalah pertanda dari bermacam-macam aktivitas yang kita lihat hari ini di *World Wide Web*, yaitu perkembangan yang sangat pesat dari semua macam *people-to-people traffic.*

DARPA berinisiatif membuat program penelitian untuk mencari teknik dan teknologi untuk menghubungkan *packets network* dengan berbagai maksud pada tahun 1973. Proyek ini dinamakan *Internetting project* dan sistem jaringan yang dibentuk oleh peneliti dinamakan *Internet.*[11] Sistem protokol yang dikembangkan melalui penelitian ini dikenal sebagai *TCP/IP Protocol suite.*[12]

Vint Cerf dan **Bob Kahn** mempublikasikan *A Protocol for Packet Network Interconnection* yang merupakan rincian desain *dari Transmission*

---

10 John Vittal juga mengembangkan MSG pada tahun 1975 sebagai program e-mail pertama yang menyediakan di dalamnya replying, forwarding dan filing capabilities, dan untuk pertama kalinya Ratu Elizabeth II dari Inggris mengirimkan e-mail pada 26 Maret 1976 dari Royal Signals and Radar Establishment (RSRE) di Malvern. *Ibid.*

11 John Quarterman menamakan Net dengan The Matrix sedangkan Tracy LaQuey mengatakan *The Matrix is sometimes calle the Net by citizens of all networks. This term is ambiguous because it doesn't refer to any one network, but works well in referring to the overall worldwide situation. If you hear someone say he's "on the Net," it propably means he can be contacted by email.* Henry Edward Hardy, *op.cit.*

12 *A Brief History of the Internet and Related Nerworks*, dapat dijumpai di http://www.isoc.org/internet/history/cerf.html. Lihat juga Barry M. Leiner, et.al., *A Brief History of the Internet*, English version, dapat dijumpai di http://www.isoc.org/internet/history/brief.htm

Control Protocol (TCP) di IEEE Transaction and Communications pada Mei 1974. Ini merupakan spesifikasi pertama dari protocol TCP yang dipublikasikan sebagai catatan percobaan internet pada Desember 1975.

Usaha untuk mengimplementasikan TCP dilakukan di Stanford, BBN dan University College of London. Dari sini terlihat usaha-usaha untuk mengembangkan protokol internet secara internasional dimulai. Percobaan TCP yang pertama yang dilakukan oleh ketiga lembaga tersebut berupa hubungan satelit melewati dua lautan (dari Hawaii ke London). Setelah percobaan itu, **Cerf** dan **Kahn** berusaha keras untuk menyelesaikan protokol internet. Desain asli dari protokol itu tidak membedakan antara TCP dan IP, yang ada hanya TCP. Pemisahan TCP menjadi TCP dan IP terjadi pada Maret 1978.

Hampir bersamaan dengan publikasi TCP itu, BBN membuka Telenet, pelayanan data paket publik (*public packet data service*) yang pertama sebagai versi komersial dari ARPANET. Sementara itu pada tahun 1975 ARPANET untuk pertama kali membuka *mailing list* yang dinamakan *MsgGroup* yang dibuat oleh **Steve Walker**. **Einar Stefferud** segera mengambil alih sebagai moderator yang pada mulanya tidak bisa dijalankan secara otomatis. Sementara itu manjemen operasional internet dialihkan dari DARPA ke *Defense Communication Agency* (sekarang *Defense Information System Agency*) sebagai jaringan operasional.

Perhatian terhadap internet pada tahun-tahun selanjutnya semakin besar, hal ini terbukti dari berbagai organisasi baru yang didirikan. Pada tahun 1979, diadakan pertemuan antara University of Wisconsin, DARPA, National Science Foundation (NSF) dan ahli-ahli komputer dari banyak universitas untuk

mendirikan *Computer Science Research* yang diorganisasikan oleh **Larry Landweber**. USENET[13] juga didirikan dengan menggunakan UUCP[14] antara Duke dan UNC oleh **Tom Truscott, Jim Ellis** dan **Steve Bellovin**. Semua kelompok asli USENET di bawah hirarki *.net.* ARPA juga mendirikan Internet Configuration Control Board (ICCB).

Kemudian pada tahun 1981 berdiri BITNET, akronim dari *Because It's Time NETwork* yang dimulai sebagai jaringan kerjasama di City University of New York dengan koneksi pertama ke Yale. Masih di tahun 1981, CSNET (Computer Science NETwork) didirikan oleh kerjasama ilmuwan komputer dan University of Delaware, Purdue Univ, Univ. of Wisconsin, RAND Corporation dan BBN dengan jaminan uang dari NSF untuk menyediakan layanan jaringan (khususnya email) kepada ilmuwan yang tidak dapat mengakses ARPANET. CSNET kemudian dijadikan sebagai *The Computer and Science Network.*[15] BITNET dan CSNET kemudian bergabung membentuk CREN (*Consortium for Research and Education Network*) pada tahun 1989.

Tahun 1982, DCA dan ARPA mendirikan *Transmission Control Protocol* dan *Internet Protocol* sebagai rangkaian protokol yang dikenal sebagai TCP/IP untuk ARPANET.[16] Setelah penggunaan TCP/IP ini oleh ARPANET,

---

13 USENET (Users' Network) merupakan Newsgroup. Bulletin Board System populer untuk sistem komputer berbasis Unix ini telah dihubungkan dengan Internet dan jaringan komputer lainnya sehingga pengguna bisa membaca dan menjawab pesan-pesan dari pada individual dari komputer lain. Lihat Kamus Istilah Internet, Andi Yogyakarta - Wahana Komputer Semarang, 2000, hal. 122.

14 UUCP (Unix-toUnix CoPy) ini pertama kali dikembangkan oleh AT&T Bell Labs pada tahun 1976 dan didistribusikan dengan UNIX satu tahun kemudian. Robert Zakon, *op.cit*

15 Lihat juga A Brief History of the Inernet and Related Networks, *op.cit*

16 Dari peristiwa ini menunjukkan salah satu dari definisi pertama tentang internet sebagai seperangkat koneksi pada jaringan khususnya yang menggunakan TCP/IP dan Internet sebagai koneksi internet melalui TCP/IP. Robert Zakon, *op.cit*

DoD mengumumkan bahwa TCP/IP menjadi standar untuk DoD. Sementara itu di Eropa dibentuk EUnet (European UNIX Network) untuk menyediakan layanan e-mail dan USENET. EUnet ini aslinya adalah koneksi antara Belanda, Denmark, Swedia dan Inggris.

ARPANET menempati garis depan dalam pengembangan internet akhirnya pada tahun 1983 dipecah menjadi dua yaitu ARPANET dan MILNET yang kemudian disatukan dengan *Defense Data Network* yang dibuat pada tahun sebelumnya. Sejumlah 68 node dari 113 node yang terhubung ke ARPANET bergabung dengan MILNET. Masih di tahun yang sama organisasi serupa BITNET muncul di Eropa dengan nama EARN (European Academic and Research Network) dengan *gateway* yang dibiayai oleh IBM. Pada tahun ini juga dikembangkan FidoNet oleh **Tom Jennings**. FidoNet adalah suatu jaringan yang menyediakan hubungan ke Bulletin Board System (BBS/Papan Berita Elektronik).

Tahun 1984 ditandai dengan diperkenalkannya *Domain Name System* (DNS) dan peluncuran novel *Neuromancer* karya **William Gibson** yang pertama kali mengenalkan istilah *cyberspace*. Jumlah host pada tahun ini mencapai 1000. Peristiwa lain pada tahun ini adalah didirikannya JUNET (Japan Unix Network) yang menggunakan UUCP dan JANET (Joint Academic Network) di Inggris yang menggunakan *Coloured Book Protocols* yang sebelumnya dikenal dengan nama SERCnet.

Sebagai kelanjutan diperkenalkannya DNS, pada tahun 1985, Information Science Institute (ISI) di UCS diberi tanggung jawab mengatur DNS

oleh DCA dan SRI untuk registrasi DNS NIC. Simbol *.com* menjadi domain pertama yang terdaftar pada 15 Maret 1985. DNS yang lainnya adalah *cmu.edu, purdue.edu, rice.edu, ucla.edu* (April), *scc.gov* (Juni) dan *mitre.org.uk* (Juli).

NSFNET dibentuk dengan *backbone* berkecepatan 56Kbps pada tahun 1986. NSF mendirikan 5 (lima) pusat super komputer yang menyediakan komputer berkekuatan besar (JVC@Princeton, PSC@Pittsburg, SDSC@UCSD, NCSA@UIUC, Theory Center@Cornell). Pendirian NSFNET diikuti dengan ledakan koneksi khususnya dari kalangan universitas. NSF juga membiayai operasional SDSCNET, JVNCNET, SURANET dan NYSERNET. Tahun berikutnya NSF menandatangani perjanjian kerjasama untuk mengelol backbone NSFNET dengan Merit Network Inc. (IBM dan MCI terlibat dalam perjanjian pengelolaan ini melalui perjanjian dengan Merit) Merit, IBM dan MCI kemudian mendirikan ANS.[17] Pada tahun 1987 ini jumlah *host* yang tercatat mencapai 10.000 dan jumlah *host* BITNET mencapai 1000.

UUNET, sebuah pusat distribusi utama untuk *UseNet news* merupakan satu dari beberapa provider layanan ke Internet didirikan pada tahun 1987. UUNET didirikan dengan dana Usenix yang menyediakan UUCP komersial dan akses Usenet. UUNET ini aslinya adalah hasil dari percobaan yang dilakukan oleh **Rick Adams** dan **Mike O'Dell**.

Tanggal 2 November 1988 ditemukan internet *worm* yang bersembunyi dalam internet. *Moris* worm ini merusak 6.000 host dari 60.000 yang ada di

---

[17] Dalam kerjasama antara IBM, Merit dan MCI, IBM mengembangkan router software sedangkan Len Bozack mengembangkan Cisco System. Klien pertamanya adalah Hewlett-Packard. Di samping membangun gateway (routers), BBN tidak percaya pasaran router sehingga dia tidak ikut dalam kompetisi dengan Wellfeet, ACC, Bridge, 3COM, Cisco dan lainnya. Vint Cerf as told to Bernard Aboba, *op.cit*

Internet. DARPA merespon hal ini dengan membentuk *Computer Emergency Response Team* (CERT). *Worm* ini menjadi pembicaraan yang hangat pada tahun itu.

Perkembangan internet di Eropa juga terus berlanjut dengan terbentuknya RIPE (*Reseaux IP Europeans*) yang dibentuk oleh *European Service Provider* untuk menjamin koordinasi administrasi dan teknik dalam mengikuti *pan-European IP Network*. Sementara itu di Amerika Serikat untuk pertama kalinya terjadi *relay email* perdagangan melalui internet yang dilakukan oleh MCI Mail melalui Corporation for the National Research Initiative (CNRI) dan Compuserve melalui Ohio State University. Jumlah host yang telah terhubung ke internet pada tahun 1989 ini mencapai 100.000 host.

ARPANET yang telah berusia 20 tahun dan baru saja diperingati ulang tahunnya oleh UCLA, berhenti keberadaannya atau dengan kata lain dibubarkan pada tahun 1990. Tahun 1990 ini juga ditandai dengan didirikannya Electronic Frontier Foundation (EFF) oleh **Mitch Kapor**. *Archie* salah satu program perangkat lunak pencari file yang dapat diterima lewat *File Transfer Protocol* (FTP) pada internet juga mulai diperkenalkan oleh **Peter Deutsch, Alan Emtage** dan **Bill Heelan** di McGill. Menyusul *Hytelnet* yang diperkenalkan oleh **Peter Scott** dari Univ. of Saskatchewan.

Perhatian terhadap pemanfaatan untuk kepentingan komersial mulai terlihat pada tahun ini sebagai konsekuensi dari inisiatif NSFNet. Selain usaha komersial, juga dibuat saluran untuk penyedia layanan informasi yang tidak komersial (nonprofit). Pada saat itu juga Dow Jones Telebase, Dialog, CARL, National Library of Medicine dan RLIN mulai *online. The World comes on-line*

(world.std.com) menjadi penyedia internet komerisal pertama yang dapat diakses.

Sebagai kelanjutan dari perkembangan internet yang mulai merambah dunia perdagangan, Commercial Internet eXchange (CIX) Association, Inc dibentuk oleh General Atomic (CERFnet), Performance Systems International, Inc (PSInet) dan UUNET Technologies, Inc. (AlterNet). Pembentukan CIX dilakukan setelah NSF membatasi penggunaan internet untuk kepentingan komersial pada tahun 1991.

Perkembangan software yang dipakai dalam internet juga terus berlanjut dengan diperkenalkannya *Gopher*[18] oleh **Paul Lindner** dan **Mark P. McCahill** dari Univ. of Minnesota tahun 1991. Masih di tahun yang sama, World-Wide Web (WWW) juga diperkenalkan olen CERN di mana **Tim Berners-Lee** sebagai pengembangnya. Sementara itu lalu lintas yang terjadi di NSFNET pada tahun ini mencapai 1 triliun bytes/tahun dan 10 bilion packet/bulan.

Seiring dengan ledakan penggunaan internet, pengguna internet membutuhkan pengakuan dari masyarakat. Pengguna internet membutuhkan pengakuan bahwa mereka itu ada, mempunyai perbedaan kepentingan dan bertanggungjawab atas kelangsungan kesehatan jaringan. Melihat keadaan tersebut maka pada Januari 1992 dibentuk Internet Society (ISOC).[19] Secara

---

[18] Gopher merupakan sistem penampilan dan pengaksesan informasi di Internet yang disusun secara hirarkis dan terstruktur sehingga mempermudah pemakai untuk mencari dan mendapatkan informasi yang diinginkannya. Gopher merupakan dasar pengembangan sistem World Wide Web. Kamus Istilah Internet, *op.cit.*, hal. 38

[19] Ide pembentukan ISOC telah didiskusikan dalam pertemuan Internet Activities Board (IAB) dan Internet Engineering Task Force (IETF) pada tahun 1991 dan pada waktu itu peresmiannya direncanakan pada INET Conference padal bulan Juni 1991 di Copenhagen, Denmark. Tetapi rencana ini meleset sehingga baru pada Januari 1992 ISOC baru berdiri. IAB yang ikut

resmi ISOC dibentuk pada Januari 1992 dan pertemuan tahunan Internet Society (INET'92) yang pertama diadakan di Kobe, Jepang. Pada pertemuan itu diusulkan sebuah asosiasi yang berada di bawah atau menjadi bagian dari ISOC dan dinamakan Internet Architecture Board (IAB).[20] Bersamaan dengan itu di Eropa, RIPE Network Coordination Center (NCC) dibentuk pada bulan April. NCC menyediakan pendaftaran alamat dan koordinasi pelayanan untuk Masyarakat Internet Eropa.

InterNIC yang dibuat oleh NSF menyediakan pelayanan khusus internet pada tahun 1993, meliputi pelayanan untuk directory and database services (AT&T), registration services (Network Solution Inc.) dan information services (General Atomics/CERFnet). Pada tahun ini jug Pemerintah Amerika membuka on-line untuk umum. Langkah ini kemudian diikuti oleh negara-negara lain pada tahun berikutnya. Amerika juga membuat peraturan yang mengatur tentang internet dengan nama US National Information Infrastructure Act. Sementara itu dunia bisnis dan media mulai memberikan perhatian pada Internet. Masyarakat mulai memasang dan berhubungan langsung dengan Internet tahun 1994. Sementara itu lalu lintas di NSFNET pada tahun ini sudah mencapai 10 triliun bytes/bulan.

Sementara itu setelah World-Wide Web (WWW) diperkenalkan pada tahun 1991, tiga tahun kemudian WWW melebihi telnet dan menduduki

---

mendiskusikan ide pembentukan ISOC didirikan pada tahun 1983 untuk menggantikan peran Internet Configuration Control Board (ICCB) dan IETF bersama dengan Internet Research Task Force (IRTF) berada dibawah IAB pada tahun 1986.

[20] ISOC dibentuk oleh orang-orang yang telah lama terlibat dalam IETF. Sebagai hasilnya adalah salah satu prinsip yang rasionaluntuk menyediakan sendiri suatu lembaga yang membantu dana dalam proses standar internet. Uraian lebih lengkap dapat dibaca pada Vint Cerf, *IETF and ISOC*, dapat dijumpai di http://www.isoc.org/internet/history/ietfhis.html. last updated 16 Oktober 1995

peringkat kedua sebagai *most popular service* di internet di belakang *ftp-data.* WWW baru bisa melebihi ftp-data pada bulan Maret 1995 untuk pelayanan dengan lalu lintas terbaik pada NSFNet yang didasarkan pada perhitungan packet dan pada bulan April 1995 berdasarkan perhitungan *bytes.* Survei ini didasarkan pada persentase lalu lintas distribusi packet dan *bytes* yang ada di NSFNet.[21]

Di Eropa sendiri pada waktu itu berusaha untuk mempromosikan teknologi informasi ini secara internasional dengan dibentuknya Trans-European Research and Education Network Association (TERENA). TERENA ini merupakan merger dari RARE dan EARN yang merupakan perwakilan dari 38 negara seperti CERN dan ECMWF. TERENA's bertujuan untuk mempromosikan dan berpartisipasi dalam pengembangan infrastruktur informasi dan telekomunikasi kualitas tinggi secara internasional untuk pemanfaatan penelitian dan pendidikan.

NSFNET melakukan langkah mundur dengan kembali menjadi jaringan penelitian pada tahun 1995. Lalu lintas utama *backbone* Amerika Serikat sekarang kembali melalui interkoneksi jaringan provider. NSFNET baru ini lahir sebagai NSF yang berdiri dengan *very high speed Backbone Network Service* (vBNS) dengan saluran pusat super komputer NCAR, NCSA, SDSC, CTC dan PSC

---

[21] Sejarah lahirnya WWW sebenarnya tidak dimulai pada tahun 1991, tetapi jauh sebelum itu langkah-langkahnya telah ditempuh untuk mewujudkannya. Seperti banyak penemuan besar, penemuan WWW didasarkan pada peristiwa yang dikelompokkan menjadi dua, yaitu pengembangan hypertext atau computer-aided reading pada dokumen elektronik dan pengembangan internet protokol yang membuat jaringan global memungkinkan. Robert Cailliau, A Short History of the Web, WebCore Disemination, IW3C2, Paris, 2 November 1995 dapat dijumpai di http://www.inria.fr/Actualitas/Cailliau-fra.html

Domain Name System (DNS) yang pada awalnya dapat diperoleh secara gratis dalam perkembangannya tidak gratis lagi. Biaya DNS yang semula disubsidi oleh NSF, mulai pada 14 September 1995 ditentukan biaya tahunan 50 dollar sedangkan NSF tetap membayar domain *.edu* dan sementara domain yang berbasis *.gov*.[22] Selama tahun 1996 ada 9.722 organisasi ditemukan tidak terdaftar setelah InterNIC menghentikan pelayanan bagi mereka sebagai akibat tidak membayara biaya *domain name*.

Tahun 1996 secara kontroversial ditandai dengan penetapan *US Communication Decency Act* (CDA) sebagai undang-undang. Undang-undang ini melarang distrbusi materi yang tidak sopan melalui internet. Beberapa bulan kemudian panel tiga hakim memberikan keputusan melawan pelaksanaan undang-undang itu. Mahkamah Agung Amerika dengan suara bulat menyatakan undang-undang itu tidak konstitusional pada tahun 1997. Selain itu tahun 1996 ini juga ditandai dengan perang WWW browser antara Nestcape dan Microsoft.

The American Registry for Internet Number (ARIN) didirikan untuk menangani administrasi dan pendaftaran anggota Internet Provider (IP) sesuai dengan daerahnya baru-baru ini dilakukan oleh *Network Solution* (InterNIC) yang dimulai pada Maret 1998. November 1998 US DoC membuat perjanjian dengan *Internet Corporation for Assigned Numbers* (ICANN) untuk melakukan proses transisi DNS dari manjemen pemerintah Amerika kepada industri .

Pengembangan internet sampai tahun 2000 terus berlangsung, baik software maupun hardwarenya, bahkan akan terus berlanjut sampai masa yang

---

[22] Untuk memperluas layanan terhadap pemakaian internet, pada tahun 1996, The Internet Ad Hoc Committee meluncurkan 7 nama generic Top Level Domain (gLTD) yaitu *.firm, .store, .web, .rec*, dan *.nom*. Robert Zakon, *op.cit*

akan datang yang akan digunakan untuk berbagai keperluan sebagaimana dikatakan oleh **Vinton Cerf** :

> It seems likely that the Internet will continue to be the environment of choice for the deployment of new protocols and for the linking of diverse systems in the academic, government, and business sectors for the remainder of this decade and well into the next.[23]

2. Cara Kerja Internet

Teknologi pokok yang melandasi semua komunikasi langsung dalam internet adalah teknologi jaringan komputer, artinya hubungan fisik antara satu komputer dengan satu komputer lain atau dengan sejumlah komputer lain. Beberapa komputer dapat dihubungkan satu dengan lainnnya melalui sambungan telepon atau melalui jaringan komputer lokal (*local area network*) yang banyak dipakai di instansi pemerintah, universitas atau perusahaan-perusahaan dan dapat juga dilakukan melalui jaringan komputer luas (*wide area network*) yang menghubungkan sejumlah komputer yang letaknya berjauhan satu sama lain.[24]

Orang yang ingin memperoleh informasi melalui komputer harus melengkapi komputernya dengan berbagai peralatan yang diperlukan.[25] Sebagai langkah awal, yang perlu diperhatikan adalah kualitas dari komputer itu sendiri. Agar bisa mengakses ke dalam jaringan komputer kita tidak perlu menggunakan super komputer yang mahal harganya. Cukup dengan komputer PC/XT dengan kapasistas minimal 268, 1Mbyte dan 40 Mbyte Harddisk, sudah dapat akses ke

---

23 Vinton Cerf sebagaimana dikatakan kepada Bernard Aboba pada bagian akhir dari *How the Internet Came to Be*, dapat dijumpai di http://www.isoc.org/internet/history/vcerf.html

24 Randy Reddick dan Elliot King, *Internet Untuk Wartawan, Internet Untuk Semua Orang*, Yayasan Obor Indonesia, Jakarta, 1996, hal, 29-30.

25 Randy Reddick dan Elliot King secara lengkap menyebutkan beberapa syarat yang harus terpenuhi agar dapat terhubung ke jaringan komputer, yaitu sebuah komputer; sambungan telepon dan sejumlah nomor telepon; modem; perangkat lunak komunikasi; rasa ingin tahu yang besar, semangat menjelajah atau kegigihan; seorang kawan yang mahir mengenai cara berhubungan dengan jaringan komputer. *Ibid*, hal. 58

internet, tetapi kapasitas komputer yang lebih besar atau semakin besar akan semakin baik.[26]

Selain seperangkat peralatan tersebut, diperlukan saluran/jaringan telepon dan *modem* agar dapat terhubung ke internet. Jaringan telepon ini dapat diibaratkan seperti kabel yang menghubungkan dua atau lebih komputer, sedangkan modem adalah sebuah alat yang dipasang pada komputer agar komputer itu dapat mengirim dan menerima data melalui kabel telepon. *Modem* mengubah informasi dari komputer ke dalam bentuk yang dapat mengalir dalam kawat telepon dan mengubah kembali informasi yang diterima melalui kawat telepon ke dalam bentuk yang dapat dipahami oleh komputer.[27]

Jenis modem yang dipakai agar komputer dapat terhubung ke internet ada dua macam, yaitu modem *internal* dan modem *eksternal*. Modem internal adalah modem yang terletak/ditancapkan di dalam CPU (*Central Processing Unit*) yang berupa *card*, tidak dapat dipindah-pindah kecuali dengan CPUnya dan modem eksternal, yaitu modem yang berdiri sendiri, terletak di luar CPU

---

[26] Onno W. Purbo, *Internet Untuk Seluruh Universitas Di Indonesia: Visi Sebuah Teknologi Merakyat*, Makalah pada Seminar Pengenalan dan Pemanfaatan Internet, Purwokerto, 15 Juni 1996, hal. 2. Bandingkan dengan pendapat Zaroni yang menyebutkan spesifikasi hardware yang dibutuhkan adalah PC 386 DX ke atas (mampu menjalankan MS-Windows pada mode enchanced) dengan RAM 4 MB atau lebih (disarankan 8 MB), Disk Drive 1.44 MB HD, 3,5" dan 1.2 MB 5.1/4", Harddisk, Mouse, dengan sistem operasi Windows 3.1 (minimal) dan MS-DOS versi 5.0. Zaroni, *Menjadi Anggota Masyarakat Virtual Bersama Wasantara-Net, Presentasi dan Demo Internet*, Makalah pada Seminra Pengenalan dan Pemanfaatan Internet, Purwokerto, 15 Juni 1996, hal. 24. Bandingkan pula dengan Randy Reddick dan Elliot King yang menyarankan penggunaan komputer macintosh lama dengan memory 512 K sudah cukup. Komputer pribadi dengan memori yang sama juga sudah cukup, lebih baik lagi jika komputer itu dilengkapi dengan hard drive, tetapi hal ini sebenarnya tidak perlu. Randy Reddick dan Elliot King, *op.cit.*, hal. 58

[27] Proses kerja modem (*MODulator* dan *DEModulator*) terdiri atas dua proses, yaitu proses *modulate* dan proses *demodulate*. Proses *modulate* terjadi pada saat pengiriman data dengan mengubah *data-data digital* (data-data *biner*) menjadi *data analog* (pulsa-pulsa suara). Proses *demodulate* terjadi pada saat penerimaan data. Proses ini mengubah kembali data analog menjadi data-data digital. Suheimi, *Kejahatan Komputer*, Andi Offset, Yogyakarta, 1991, hal. 38-39. Semua proses ini dikendalikan oleh perangkat lunak komunikasi yang memerintahkan modem untuk memutar nomor telepon atau menjawab telepon yang masuk dan melaksanakan fungsi-fungsi lain. Randy Reddick dan Elliot King, *op.cit*, hal. 30-31

dan dapat dilepas dari komputer. Modem biasanya dilengkapi dengan perangkat lunak komunikasi dan faksimile.[28] Untuk bisa akses ke internet, disarankan menggunakan modem yang memiliki kecepatan transfer data minimal 9600 bps[29]

Setelah komputer dilengkapi dengan modem dan saluran telepon, langkah selanjutnya adalah mendaftarkan diri ke penyedia jasa layanan internet (*Internet Service Provider*/ISP) untuk mendapatkan akses ke internet dengan cara berlangganan atau dapat langsung akses ke ISP yang tidak mensyaratkan pendaftaran untuk berlangganan, cukup menghubungi nomor telepon yang telah ditentukan.[30] *Internet Service Provider* adalah suatu organisasi atau perusahaan yang memberikan jasa hubungan ke internet bagi para pengguna komputer dengan menarik sejumlah biaya. ISP ini biasanya disebut *Provider* saja.[31]

Selain menggunakan alat komunikasi dengan menggunakan kabel telepon (yang dikelolaa oleh PT. Telkom) maka sekarang ISP menyediakan infrastruktur yang membuat akses ke internet lebih cepat tanpa melalui kabel telepon. Era infrastruktur internet sudah memasuki era *broadband,* baik yang lewat saluran terestrial, lewat kabel, lewat satelit atau lewat gelombang radio

---

28 Perangkat lunak apa saja yang terdapat dalam modem, secara lengkap dapat dibaca di Randdy Reddick dan Elliot King, *ibid,* hal, 60-61. Bandingkan juga dengan Suheimi, *op.cit.*, hal. 48-52. Lihat juga mengenai penjelasan istilah-istilah yang terdapat dalam modem pada Majalah Infokomputer, Edisi Internet, pada rubrik Tutorial, Memahami Istilah pada Modem, Juli-Agustus 1997, hal. 44-46. Ada tiga perusahaan terdepan yang mengembangkan teknologi modem, yaitu Robotic, Rockwell dan Lucent Tchnologies. Ketiga perusahaan ini bersaing ketat dalam memuat modem yang bisa menerima data dengan kecepatan sampai 56Kbps dan dapat mengirim dengan kecepatan sampai 33,6Kbps. Keterangan lebih jelas mengenai spesifikasi jenis modem dengan kecepatan itu dapat dibaca pada Infokomputer, Edisi Internet, pada rubrik Tips, *Perlukan Meng-upgrade Modem ke 56Kbps*, Juli-Agustus 1997, hal. 30

29 Zaroni, *op.cit.* Bandingkan dengan Randy Reddick dan Elliot King yang menyarankan modem berkecepatan 2.400 bps. Randy Reddick dan Elliot King, *op.cit.*, hal. 60

30 Untuk Indonesia penyedia layanan internet (ISP) yang tidak melalui pendaftaran untuk berlangganan dilakukan oleh TelkomNet yang dikelola oleh PT. Telkom.

31 *Kamus Istilah Internet,* Kerjasama Wahana Komputer Semarang dengan Penerbit Andi Yogyakarta, 2000, hal. 54

yang *nirkabel*. Ketika akses internet mulai memasyarakat, kecepatan akses sekitar 14,4 Kbps untuk kalangan pengguna rumahan/pribadi sudah tergolong mewah, kemudian dengan munculnya modem dengan kecepatan 28,8 Kbps dan 56 Kbps akses internet sebenarnya bisa lebih cepat, tetapi karena infrastruktur telekomunikasi Indonesia tidak mendukung akses secepat itu. Dengan adanya *broadband*, pengguna internet dimanjakan dengan akses internet yang semakin cepat mencapai *gigabit per second* dalam 24 jam tanpa biaya pulsa telepon.[32]

Langkah selanjutnya setelah (atau sebelumnya) mendaftarkan diri ke ISP adalah menyediakan *software* dalam komputer yang hendak tersambung ke internet berupa program aplikasi yang dapat digunakan untuk menjelajah belantara internet yang disebut *Browser*. Program aplikasi tersebut dapat diinstal ke dalam komputer secara tersendiri atau sudah terintegrasi bersama sistem operasi lain. *Browser* yang sekarang banyak digunakan adalah *Internet Explorer* yang terintegrasi bersama sistem operasi Windows dari Microsoft dan *Netscape Communicator* dari Netscape Corporation (sebelum dibeli oleh AOL Online).[33] Persaingan antara Internet Explorer dan Netscape menjadi persaingan dari generasi ke generasi. Browser-browser alternatif juga beredar di pasaran[34] dan

---

32 Lihat berita di Tabloid PCplus, No. 12/II/10-16 Januari 2001, dengan judul *Broadband: Lebih Besar, Lebih Mengasyikkan*, pada rubrik plusFokus, yang mencantumkan juga beberapa ISP yang menyediakan layanan broadband.hal. 16-18, dan PCplus No. 16/II/7-13 Februari 2001 dengan judul Kabelvision Merajai Internet Lewat Serat Optik, pada rubrik plusAktual, hal. 4. Hadirnya broadband atau broadband revolution yang merupakan the next revolution of internet akan semakin meningkatkan interactivity melalui internet yang dapat digunakan untuk berbagai keperluan. Lihat lebih jelas pada Dimitri Mahayana, *op.cit*, hal. 11.

33 Baca juga kelebihan dan kekurangan Netscape Communicator versi 4.0 dan Internet Explorer versi 4.0 pada Majalah Infokomputer, Edisi Internet Vol. 1 No. 4, 15 Mei-15 Juni 1997, hal. 28-41

34 Berbagai browser alternatif beredar di pasaran saat ini, seperti NeoPlanet, Netcaptor, Enigma 3.6.0, Opers 5.0 dan lain sebagainya. Browser-browser itu mempunyai kelebihan dan kekuarangan. Keterangan lebih jelas mengenai hal ini dapat dilihat di PCplus No. 15/II/31 Januari-06 Februari 2001, dengan judul *Microsoft dan Netscape: Berseteru Sampai Generasi Keenam dan berbagai Alternatif Browser*, pada rubrik plusFokus, hal. 16-19

dapat diperoleh dengan cara men*download* dari situs pencipta browser tersebut (secara gratis) atau menginstalnya dari *Compact Disk* (CD) yang dijual secara bebas di pasaran.

Memperoleh informasi melalui komputer yang terhubung melalui sistem antar-jaringan (*internetworking*) agak rumit. Sistem *internetworking* berkembang dari sistem jaringan komputer yang terus dibangun sampai sekarang. Pemerintah, perusahaan, universitas, sekelompok orang atau pribadi menghubungkan komputer mereka menjadi suatu jaringan sehingga orang dapat dengan mudah berbagi informasi dengan menggunakan program aplikasi. Jaringan ini dinamakan *Local Area Network* (LAN). Pada LAN satu komputer atau lebih berfungsi sebagai pusat untuk beberapa komputer lainnya yang dinamakan pembagi (*server*) dan umumnya berisi file yang digunakan semua orang.

Semakin luasnya jaringan menyebabkan terjadi hubungan antar server yang menggunakan sambungan data khusus dan komputer khusus yang dinamakan *router*. *Router* memiliki kemampuan melewatkan paket Internet Protocol dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur di antara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah *algoritma routing terdistribusi* untuk mementukan jalur terbaik yang dilalui paket IP dari suatu sistem ke sistem lain.[35]

---

[35] Suatu komputer dapat terhubung ke komputer lain selain menggunakan protokol TCP/IP maka diperlukan peralatan lain yang disebut network interface yang berupa card ethernet atau modem. Di luar itu diperlukan peralatan lain yaitu Device Penghubung Jaringan yang secara umum dibagi dalam beberapa kategori yaitu Repeater, Bridge dan Router. Onno W. Purbo, Adnan Basalamah, Ismail Fahmi dan Achmad Husni Thamrin, *TCP/IP Standar, Desain dan Implementasi*, Elex Media Komputindo, Jakarta, 2000, hal. 32. Lihat juga Suheimi, op.cit., hal. 56-72

Seiring dengan perkembangan teknologi, hubungan antar komputer ini tidak hanya dilakukan dengan kawat telepon, tetapi dipakai pula kawat serat optik dan teknologi lain yang memungkinkan lahirnya jalan raya informasi bebas hambatan (*superhighway*). Pengembangan jaringan besar antar-jaringan tergantung pada dua faktor. *Pertama,* hubungan fisik antar komputer, *kedua* komputer harus berbicara dalam bahasa yang sama, artinya menggunakan aturan atau protokol komunikasi yang sama untuk mengenali, menyalurkan dan mengolah informasi.[36] Sistem operasi atau software yang digunakan untuk berhubungan antara satu komputer dengan komputer lain dalam suatu jaringan bisa berbeda-beda. Perbedaan sistem operasi ini menyebabkan apabila tidak ada protokol yang mengatur menyebabkan komputer yang berbeda sistem operasinya akan mengalami kesulitan dalam berhubungan.

Untuk menangani semua masalah komunikasi data (transfer, menerima dan mengolah data) harus ada sekumpulan aturan yang harus bekerja sama satu dengan lainnya. Sekumpulan aturan itu dinamakan protokol komunikasi. Protokol ini diimplementasikan dalam bentuk program komputer (*software*) yang terdapat pada komputer dan peralatan komunikasi data lainnya. *Transmission Control Protocol/Internet Protocol* (TCP/IP) adalah sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data pada *Wide Area Network* (WAN). Komputer yang berbeda jenis dan sistem operasi bisa berkomunikasi karena menggunakan bahasa yang sama yaitu protokol TCP/IP. Sebagai contoh komputer PC (*personal computer*) dengan sistem

---

[36] Randy Reddick dan Elliot King, *op.cit.*, hal. 39

operasi Windows dapat berkomunikasi dengan komputer Macintosh atau dengan Sun SPARC yang menjalankan Solaris.[37]

Dari uraian di atas, secara ringkas dapatlah diambil kesimpulan bahwa internet tumbuh karena dua faktor. *Pertama* hubungan fisik yang terdiri dari sambungan data berkecepatan tinggi dibangun yang menghubungkan jaringan-jaringan komputer (*internetworking*) di berbagai universitas, lembaga pemerintah, perusahaan dan organisasi lain. Semua ini melahirkan *de facto* jaringan nasional. *Kedua* karena protokol TCP/IP telah luas diterima maka informasi dapat mengalir secara terbuka dalam jaringan yang saling berhubungan. Itulah yang membentuk internet walaupun komputer-komputer itu memiliki arsitektur perangkat keras dan sistem operasi yang berbeda-beda.[38]

Setelah semua persyaratan untuk hubungan ke internet seperti disebutkan di atas telah terpenuhi, maka komputer siap terhubung ke internet. Langkah pertama adalah dengan *dial-up* nomor telepon penyedia layanan internet (ISP) setelah komputer dan modem dihidupkan. Setelah menekan enter atau mengklik mouse (jika pakai) maka modem akan mengeluarkan suara yang khas yang akan menandakan saluran akan tersambung atau tidak. *Internet Service Provider* yang ada di Indonesia dalam melakukan pelayanan tidak hanya melakukan atau menyediakan layanan tersendiri. ISP lokal itu selanjutnya terhubung ke ISP Global dan inilah yang menyebabkan bisa terjadi hubungan

---

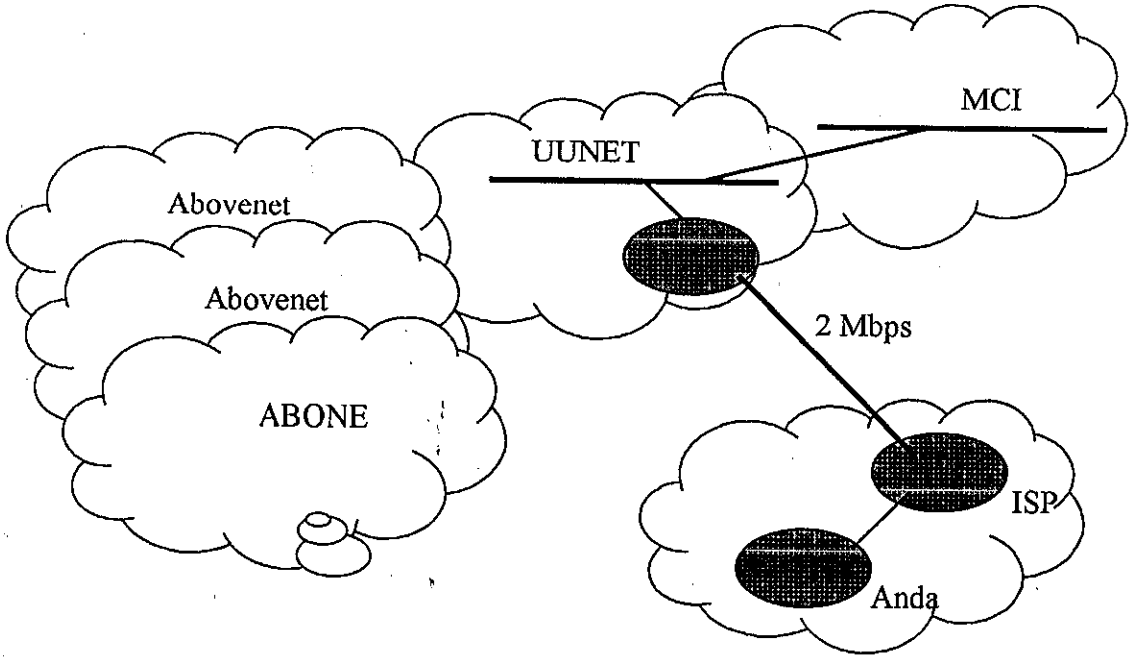
37 TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Berkat prinsip ini tugas masing-masing protokol menjadi jelas dan sederhana. Protokol yang satu tidak perlu mengetahui cara kerja protokol yang lain, sepanjang ia masih bisa mengirim dan menerima data. Onno W. Purbo, Adnan Basalamah, Ismail Fahmi dan Achmad Husni Thamrin, *op.cit.*, hal. 1 dan 22

38 Randy Reddick dan Elliot King, *op.cit.*, hal. 103-104

antar negara melalui internet. Cara kerja ISP dapat dilihat pada Gambar 1 di bawah ini.

Gambar 1

Koneksi Anda ke ISP dan ISP ke ISP Global



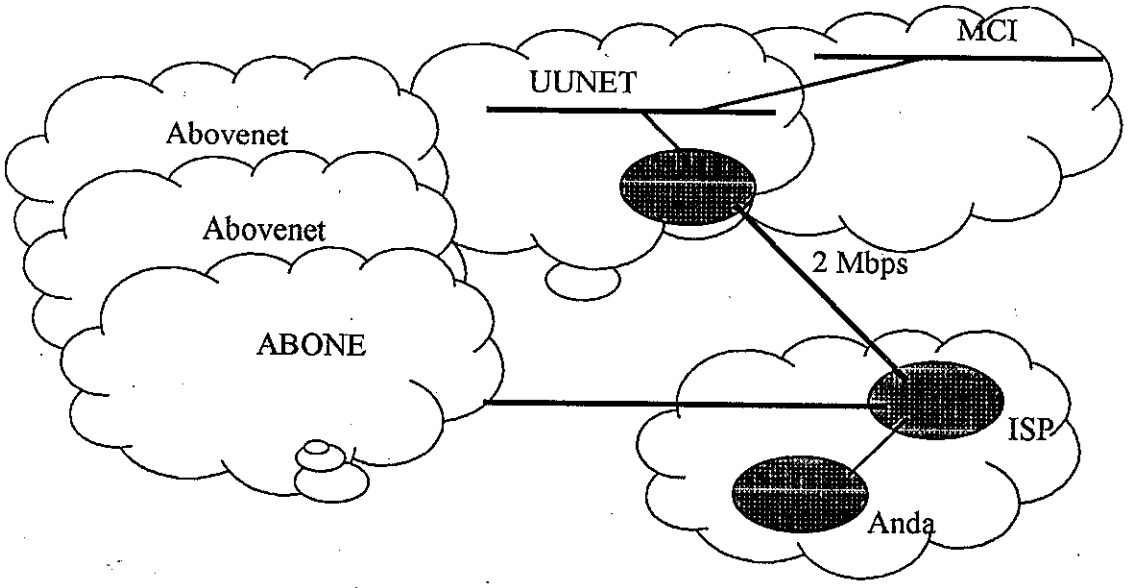
Sumber : *Rafdian Rasyid, Membongkar Rahasia ISP Anda dalam Infokomputer, Februari 2000, hal. 76*

Pada Gambar 1 terlihat bahwa pengguna internet terkoneksi ke ISP lokal dengan menggunakan *dial-up* atau *leased line* yang lebarnya misalnya 64 Kbps. ISP lokal sendiri terkoneksi ke ISP Global di USA dengan *bandwidth* 2 Mbps (*receive*) dan mungkin 1 Mbps (*transmit*). Secara umum akses yang dirasakan normal (cepat) jika *pertama* bandwidth anda ke ISP belum *overload* atau *kedua bandwidth* anda ke Internet belum *overload*. Dari gambar 1 terlihat bahwa ISP lokal hanya terhubung ke hanya satu ISP Global, maka ISP anda tersebut dikatakan *Single-Homed*. Jika terhubung ke lebih dari satu ISP Global

maka disebut *Multi-Homed*, sehingga gambarnya berupa selain terhubung ke UUNET juga dapat terhubung ke ABONET seperti terlihat dalam gambar 2.[39]

Gambar 2

ISP Anda merupakan ISP yang Multi-Homed



Sumber : *Rafdian Rasyid, Membongkar Rahasia ISP Anda dalam Infokomputer, Februari 2000, hal. 77*

ISP *Single-Home* sebenarnya tidak jelek meskipun ISP yang *Multi-Homed* hampir dipastikan baik. ISP *Single-Home* juga mempunyai keunggulan, yaitu dalam hal *load balancing*, di mana jika medium telekomunikasi keduannya menggunakan medium yang sama (misal, sama-sama *leased line*), kemudian ISP tersebut membuat *link ke Upstream Provider*-nya dengan besar *bandwidth* yang sama, maka ISP tersebut dapat menggunakan *load balancing* di tingkat *hardware* (khususnya jika meng-gunakan *router Cisco* dan dalam box yang saina). ISP yang menggunakan metode ini mendapatkan dua keuntungan yaitu

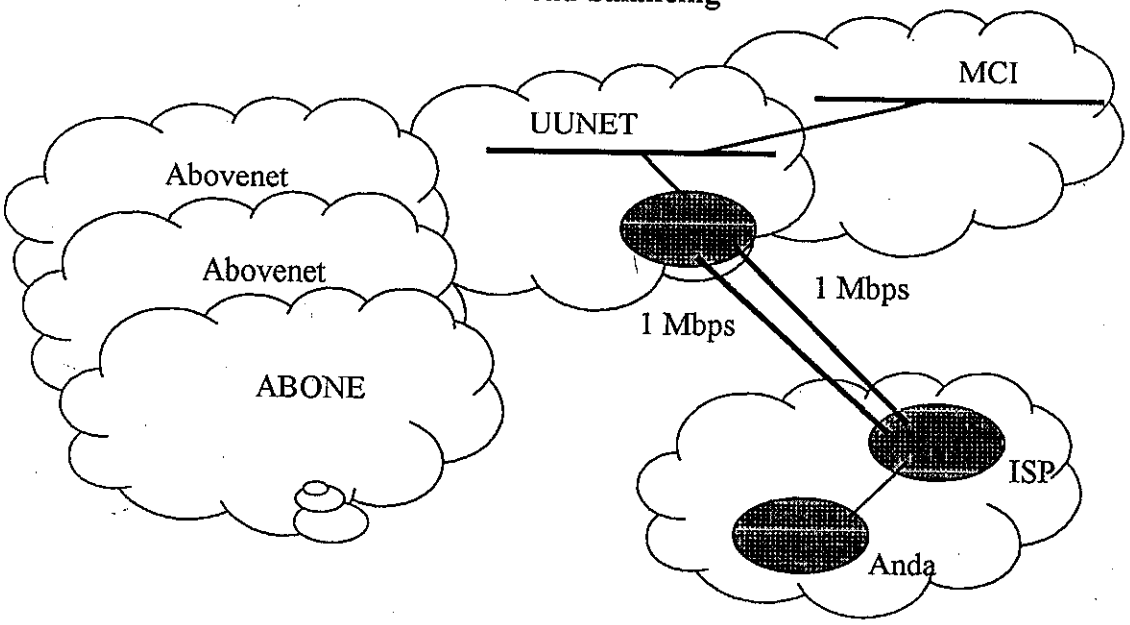
---

39 Rafdian Rasyid, *Membongkar Rahasia ISP Anda,* dalam Infokomputer, Februari 2000, hal. 76-77

redundansi dapat berlangsung, dengan kata lain jika satu link mati maka masih di*back up* oleh *link* yang satunya lagi dan sebaliknya. Kedua, dapat menerapkan *load balancing* per sesi atau per sesi TCP (dengan *Round Robin*) di tingkat hard-warenya. Jika tidak *per TCP session, load balancing* menyebabkan paket harus lewat jalur yang berbeda, sehingga urutan kedatangan paket akan berantakan dan ini tidak disukai oleh TCP. Untuk lebih jelasnya lihat gambar 3.[40]

Gambar 3

ISP yang Single-Homed dengan dual link dapat menerapkan hardware load balancing



Sumber : *Rafdian Rasyid, Membongkar Rahasia ISP Anda dalam Infokomputer, Februari 2000, hal. 78*

Jika komputer pengguna sudah connect atau terhubung ke ISP maka pengguna sudah mulai terhubung ke internet. Bagan atau struktur bagaimana cara kerja internet dapat dilihat pada gambar 4. Pengguna dapat menjalankan program aplikasi yang disediakan untuk berkomunikasi atau mencari data atau orang dalam internet. Program aplikasi yang dapat digunakan antara lain *E-mai,*

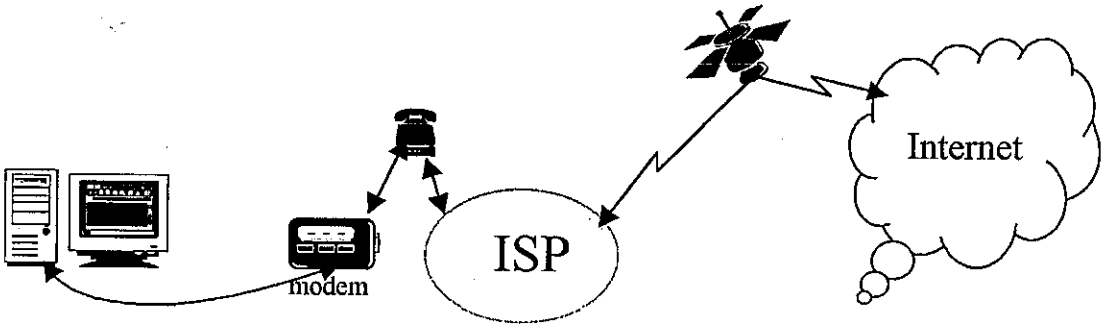
---

[40] *Ibid*, hal. 78

Telnet, FTP, Hytelnet, Archie, WAIS, Veronica dan *Jughead, Finger, Whois, Knowbot* dan *Fred, Gopher, World Wide Web, Internet Relay Chat, Newsgroup* dan *Mailing List.*

Gambar 4

Struktur Internet



Jika pengguna menggunakan *World Wide Web (WWW)* setelah komputer terhubung ke ISP maka pengguna akan menggunakan *browser* yang ada dalam komputer yang dipakai. Kemudian pada kotak *Uniform Resource Locator* (URL) dituliskan alamat virtual yang dituju. Setelah layar komputer menampakkan atau menyajikan gambar atau tulisan dari alamat yang dituju, maka pengguna siap untuk melakukan hubungan atau komunikasi dengan penghuni virtual lainnya maupun melakukan penjelajahan untuk mencari data atau file yang diperlukan.

Untuk kecepatan akses selain dengan meningkatkan kecepatan modem, maka browserpun dapat digunakan untuk mempercepat tampilan atau transfer file. Jenis perangkat lunak yang dapat digunakan untuk itu adalah *akselerator browser*. Saat ini banyak teknologi yang dapat digunakan untuk mengurangi waktu mengakses halaman Web dengan teknologi *push* dan *pull*. Tekonologi *push* sama seperti yang digunakan *PointCast Network* dari PointCast yang secara

otomatis mengirim isi Web yang sudah dibikin menurut permintaan (*personalized*) ke personal computer pengguna segera setelah mengakses internet. Teknologi *pull* memungkinkan pengguna menjelajah Web dan informasi dari situs-situs favorit dalam waktu singkat.[41]

3. Fasilitas Yang Terdapat Dalam Internet

Dalam internet manusia tidak hanya bisa berkomunikasi satu dengan yang lain, tetapi juga bisa mencari informasi, data atau program di gudang (*memori*) yang berada di pelabuhan (komputer) di pantai lautan komunikasi global bernama Internet. Internet dapat dipandang sebagai sebuah kompleks gedung perpustakaan raksasa yang sangat aneh. Di kompleks perpustakaan maya ini terdapat sebuah buku tunggal bernama WWW (World Wide Web) atau sekarang dikenal dengan sebutan web saja, terdiri dari berjuta-juta halaman, berserakan di seluruh penjuru dunia.[42]

Internet tidak hanya menyajikan informasi yang telah dikemas dan disimpan dalam sebuah *perpustakaan maya*. Internet juga dapat digunakan untuk berkomunikasi melalui fasilitas-fasilitas yang diberikan berupa *E-mail, Telnet* dan *FTP* (File Transfer Protocol) sebagai program dasar internet, *Hytelnet, Archie, WAIS, Veronica, Jughead, Finger, Whois, Knowbot* dan *Fred* yang dapat dipakai untuk mencari file dan orang. Selain itu ada pula *Gopher* dan *World Wide Web* sebagai alat-alat penjelajah dan *Newsgorup, Mailing List* dan

---

41 Uraian lebih jelas mengenai cara-cara mempercepat browser dapat dibaca pada Majalah Infokomputer, Edisi Khusus Internet, Vol. I/3, 15 April-15 Mei 1997 pada rubrik Cakrawala dengan judul *Kiat-kiat Pemercepat Browser* dan *Penggenjot Kinerja Browser*, hal. 16-18.

42 Halaman-halaman web tersebut saling berkait satu sama lain melalui yang disebut *hyperlink*, yaitu tulisan atau gambar yang ada di setiap halaman, yang merujuk ke halaman web lainnya. Web terdiri dari situs berupa kumpulan halaman web dalam satu *komputer-simpul jaringan internet* yang merujuk satu sama lainnya melalui hyperlink dan juga merujuk situs-situs lain di komputer lain di negara lainnya. Dengan demikian internet dapat diibaratkan sebagai sebuah gedung perpustakaan maya. Armahedi Mahzar, *loc.cit.*, hal. 10-11

Internet Relay Chat dan *Voice over Internet Protocol (VoIP)* sebagai aplikasi interaktif di internet.

E-mail atau surat elektronik dapat digunakan untuk mengirim dan menerima pesan pribadi maupun publik. *E-mail* menjadi alat komunikasi yang paling mudah dan efisien dibandingkan dengan pesawat telepon. *E-mail* pada dasarnya tidak ada bedanya dengan mengirimkan surat biasa melalui pos (yang dijuluki oleh pengguna *e-mail* dengan nama *pos bekicot* karena kelambanan pelayanan dalam penyampaian surat). Bedanya *e-mail* dan surat biasa adalah pada *e-mail* pesan dikirimkan dari sebuah komputer dan diterima oleh sebuah komputer.

E-mail memiliki berbagai kelebihan dibandingkan dengan *pos bekicot*. *E-mail* memiliki kelebihan dalam hal kecepatan dan kemudahan. Perangkat *e-mail* memungkinkan pengguna menjawab pesan-pesan secara otomatis cukup dengan menekan beberapa tombol saja atau seperti pada pesawat telepon ada mesin penjawab e-mail jika pemilik e-mail tidak punya waktu untuk menjawab e-mail-e-mail yang masuk. Kelebihan selanjutnya adalah *e-mail* bersifat tidak resmi, hal ini menyebabkan *e-mail* tidak tersentuh birokrasi yang rumit seperti surat biasa.[43]

Salah satu daya tarik *e-mail* adalah ia tidak menganggu seperti telepon. Kita tidak dikejutkan oleh bunyi dering telepon ketika kita sedang tidur atau tidak pula dibuat penasaran oleh penelepon yang salah sambung. Pengguna e-mail dapat memproses secara leluasa dan menjawab pesan-pesan tanpa melalui

---

[43] Randy Raddick dan Elliot King, *op.cit.*, hal. 132-134. Lihat juga Irvan Nasrun, *Memanfaatkan E-mail Pada Kondisi Darurat*, dalam majalah Infokomputer, edisi Internet, Vol. 1 No. 6, 15 Juli-15 Agustus 1997 hal. 15-18.

pengawasan orang lain pada waktu dan tempat yang disukainya, baik di rumah, kantor ataupun warung internet. *E-mail* naik daun karena ia merupakan *medium asinkron* dan dapat dibaca oleh komputer. Komputer berperan penting karena agen antarmuka akan menggunakan bit-bit itu untuk memprioritaskan dan mengirim pesan-pesan secara berbeda.[44]

Meskipun *e-mail* mempunyai beberapa kelebihan dibandingkan dengan pos biasa, tetapi *e-mail* juga memiliki kerumitan-kerumitan. Kerumitan yang pertama adalah berkaitan dengan tersedianya perangkat lunak. Di samping perangkat lunak yang digunakan untuk menulis pesan, mengirimkan atau membaca dan mengelola pesan-pesan yang masuk, mungkin masih diperlukan beberapa perangkat lunak komunikasi yang ada dalam komputer pribadi atau menggunakan perangkat lunak jaringan atau *mail utility* yang berjalan dalam komputer lain yang sama sekali asing.[45] Kerumitan ini sebenarnya sekarang tidak perlu dirisaukan karena begitu kita membeli komputer dan berlangganan internet lewat Internet Service Provider maka fasilitas tersebut sudah masuk dalam komputer yang dibeli dan jikapun belum ada maka oleh pihak penjual komputer atau pengelola ISP akan dipasangkan.

Kerumitan yang kedua adalah memberi alamat. Meskipun Internet memiliki format standar untuk alamat, seorang pemakai dapat mengirim pesan pada orang yang berada di luar jaringan Internet. Internet dan berbagai program e-mail masing-masing memiliki caranya sendiri untuk memberi tahu ke mana pesan harus dikirimkan. Kerumitan yang ketiga adalah soal lingkup pribadi dan keamanan. Pesan *e-mail* dapat dibaca lebih dulu oleh pengelola sistem komputer

---

44 Nicholas Negroponte, *Being Digital, Menyiasati Hidup Dalam Cengkraman Sistem Komputer,* Mizan, Bandung, 1998, hal. 169-170

45 Randy Raddick dan Elliot King, *op.cit*, hal. 134

dan pengelola dapat memilih pesan-pesan yang akan diteruskan.[46] *E-mail* yang telah dikirim akan melewati jalan raya bebas hambatan, dan di jalan raya bebas hambatan ini tidak ada jaminan keamanan, artinya pesan atau paket-paket yang dikirim bisa saja dibajak atau dihentikan di tengah jalan oleh orang lain yang sama-sama menggunakan jaringan itu. Dapat juga terjadi pesan yang dikirim atau disampaikan itu tidak sesuai dengan apa yang diinginkan karena kemungkinan isinya telah diubah oleh pembajaknya.

Persoalan keamanan pada *e-mail* bisa diatasi dengan mengaplikasikan program *Pretty Good Privacy* (PGP) yang menjadi standar *de facto* untuk masalah *enkripsi* informasi (terutama *e-mail*). PGP yang dibuat oleh **Phill Zimmermann** adalah program enkripsi yang memiliki tingkat keamanan cukup tinggi dengan menggunakan *private-public key* sebagai dasar otentifikasinya.[47]

Format utama *e-mail* berupa teks. Dengan adanya fasilitas *attachment* pada aplikasi *e-mail*, maka pengguna *e-mail* bisa mengirim atau menerima file dalam format dokumen (doc), *spreadsheet*, suara, klip gambar bergerak atau video bahkan aplikasi software yang dipadatkan atau dikompresi.[48]

Selain *e-mail*, program dasar yang dapat dipakai adalah *Telnet*. *Telnet* merupakan fasilitas yang memungkinkan para pengguna komputer untuk menghubung atau terhubung ke suatu komputer server di internet dan mengakses segala fasilitasnya seakan-akan pengguna tersebut berada di depan komputer

---

[46] *Ibid*, hal.135

[47] Joko Yuliantoro dan Onno W. Purbo, *PGP Sebagai Pengaman E-mail Anda*, dalam Majalah Infokomputer, Edisi Internet, Vol. 1 No. 4, 15 Mei-15 Juni 1997, hal. 42-47

[48] Alois Wisnuhardana, *Mempelajari dan Memahami Attachment E-mail*, dalam Tabloid PCplus pada rubrik plusBelajar, hal. 5

server tersebut secara langsung.[49] Dengan *Telnet* maka seseorang yang berada jauh dari kantornya dapat mengakses data yang ada di jaringan komputer di kantor.[50]

Pada mulanya program *Telnet* digunakan untuk melakukan *login* secara *remote* pada sistem operasi UNIX. Dengan menggunakan program *Telnet*, pengguna dapat mengakses *login* pengguna di suatu komputer dari komputer lain. *Telnet* merupakan program lintas sistem operasi karena dapat dijalankan untuk melakukan *remote login* dari sistem operasi yang berbeda. Misalnya komputer dengan sistem operasi *Slackware* LINUX dapat di*remote login* dari komputer dengan sistem operasi FreeBSD UNIX. Tetapi tidak semua komputer mendukung *remote login* dan biasanya hanya sistem operasi UNIX yang mendukung login dari jarak jauh.[51]

Telnet merupakan alat internet yang paling sederhana dari semua alat internet. Meskipun sederhana, *Telnet* mempunyai tiga kelemahan, yaitu :

1. Alamat dan cara masuk situs yang akan dikunjungi harus diketahui lebih dahulu
2. Sebagian besar situs hanya mengijinkan orang melihat-lihat file teks. Ada juga yang mengijinkan orang mengirimkan atau mengambil file, tetapi menyalin file *binary* merupakan tugas FTP
3. Indeks situs *Telnet* dalam jaringan komputer terbatas dan situs tidak akan ditemukan jika cara yang biasa yang digunakan untuk mencarinya.

---

49 Kamus Istilah Internet, hal. 114

50 Baca juga Infokomputer Vol. XI No. 8 Agustus 1995 dengan judul *Tetap Terkoneksi Ke Jaringan*, hal. 46-47.

51 Yus Dwi Handoko, *Memanfaatkan Program Telnet*, Majalah Infokomputer Vol. XIV No. 02 Februari 2000, hal. 117

Untuk menemukan situs yang mengandung bahan yang digunakan maka dapat dipakai *Gopher*, World Wide Web, Mailing List, Newsgroups atau Hy*telnet*.[52]

FTP berarti *File Transfer Protocol* (protokol pemindahan file). Nama ini diberikan para pembuat program komputer pada serangkaian konvensi yang memungkinkan satu jenis komputer menggunakan perangkat aturan sendiri untuk mengirimkan atau menerima file ke atau dari suatu komputer jenis lain yang menggunakan perangkat aturan yang juga lain.. Misalnya komputer UNIX yang dihubungkan dalam jaringan melalui komputer VAX yang menjalankan VMS, dapat bertukar file dengan komputer besar IBM yang bekerja di bawah aturan yang lain dan kemudian menyalurkan file ke komputer Macintosh pengguna.[53]

FTP memudahkan pemindahan file dari satu komputer ke komputer lain dan sudah menjadi bahasa baku untuk berbagai data. Cara menghubungi FTP persis sama dengan cara menghubungi *Telnet*. Berbeda dengan *Telnet* yang mengharuskan pengguna memiliki kata sandi untuk masuk *remote computer*, FTP *anonymous* menjadikan siapa saja yang menggunakan atau berada pada internet dapat mengalihkan file (dari dan kadang-kadang) ke *remote computer* dengan hanya menyebutkan kata *anonymous* sebagai kata sandi identitas pengguna.[54]

---

52 Randy Raddick dan Elliot King, *op.cit, hal. 174-175* Untuk mencari file yang hendak didownload atau ditransfer, maka file tersebut harus dicari (jika belum tahu). Cara mencarinya adalah dengan menggunakan search engine yang bernama FTPsearch. Mengenai bagaimana mencari file dengan fasilitas FTPsearch khususnya dengan ftpsearch.lycos.com dapat dibaca tulisan Yus Dwi Handoko, *Mencari File di Internet*, Majalah Internet, Edisi 15 November-15 Desember 2000, hal. 63-65

53 Randy Raddick, *Ibid, hal.* 246

54 *Ibid, hal.* 116

Di antara semua protokol internet, FTP barangkali merupakan protokol yang paling tidak ramah pada pengguna. FTP bukan alat penjelajah yang terlalu ramah dan efisien. Sikapnya yang *strictly business*, tidak main-main dan pengguna dianggapnya sudah tahu prosedur. Untungnya tidak banyak prosedur yang harus dipelajari. Prosedur itu mencakup berhubungan dan memutuskan hubungan, memperoleh dan membaca *direktori*, berpindah-pindah antara direktori dan mengambil file dengan protokol yang seharusnya.[55]

Penggunaan FTP yang paling populer saat ini adalah untuk meng-*upload* atau men-*download* file-file yang digunakan untuk menyusun *Website*. File yang diperlukan agar suatu halaman atau situs bisa tampil sempurna harus berada dalam *Web server* yang sudah ditentukan. FTP dalam hal ini menjadi salah satu alat bantu yang harus dipunyai untuk memperlancar proses penyusunan *homepage*.[56]

Selain perangkat lunak program-program dasar seperti yang disebutkan di atas, ada juga perangkat lunak untuk mencari file dan orang. *Hytelnet* adalah salah satunya. *Hytelnet* diperlukan untuk memecahkan masalah kelemahan yang ada pada *Telnet*, yaitu pertama, pengguna harus tahu prosedur *log-in* untuk tiap-tiap situs yang ingin pengguna hubungi. Kedua, setiap situs memiliki menu dan perintah yang berbeda. *Hytelnet* menaruh *menu interface* pada situs *Telnet* yang terbuka untuk umum dan membantu mengadakan hubungan pada situs-situs jauh. Jika internet pengguna atau *host internet* pengguna tidak memiliki

---

55 Randy Raddick dan Elliot King, *op.cit, hal.* 246-247 dan 253.

56 FTP sering digunakan oleh kalangan perguruan tinggi maupun peneliti bahkan perseorangan. Teknik transfer file dengan menggunakan FTP dapat dibaca dalam tulisan F.X. Bambang Irawan, *Urusan Transfer File Butuh FTP*, Tabloid PCplus, No. 15/II/31 Januari-06 Februari 2001, hal. 6

perangkat lunak *client*[57] *hytelnet*, pengguna dapat masuk perangkat lunak client *hytelnet* melalui *Telnet*.[58]

Perangkat lunak pencari file dan orang yang lain adalah *Archie*. *Archie* dan FTP adalah dua sejoli, seperti saudara sepupu dari majalah komik *Veronica* dan *Jughead*. *Archie* adalah detektif jaringan. *Archie* menelusuri indeks pangkalan data dan arsip dengan kata kunci yang pengguna berikan. *Archie* kembali dengan daftar direktori dan file nama yang mengandung kata yang pengguna berikan. Daftar file dan direktori ini disusun oleh *host site*. Jika *host site* pengguna pengguna tidak mempunyai client *Archie* dan komputer pengguna juga tidak ada, maka ada dua pilihan untuk menghubungi client *Archie* untuk umum. Pertama, menggunakan salah satu dari alat penjelajah jaringan seperti *Hytelnet*, *Gopher*, atau World Wide Web. Kedua, pengguna dapat menggunakan *Telnet* untuk menjangkau client *Archie*.[59]

Veronica (*Very Easy Rodent-Oriented Netwide Index to Computerized Archiver*) dan Jughead adalah program untuk mencari file yang dapat dilihat melalui perangkat lunak *Gopher*. Kedua program ini mencari direktori-direktori dari ribuan situs *Gopher* di seluruh dunia. Salah satu keunggulan Veronica adalah memungkinkan kita mempersempit bidang informasi yang dicari dengan menggunakan *logika Boolean* (AND, OR, NOT). Kerja Jughead sama dengan kerja Veronica bahkan jika pengguna mencari situs dengan Veronica maka hal tersebut dapat juga dilakukan dengan Jughead dan mendapat hasil yang sama, tidak ada perbedaan. Namun ada perbedaan tipis di antara keduanya dalam hal

---

57 Client adalah program aplikasi perangkat lunak yang mengambil jasa dari sebuah server dalam jaringan. Client menyusun informasi yang dihimpun dari tempat lain dalam jaringan dan interface bagi pengguna.

58 Randy Raddick dan Elliot King, *op.cit, hal.* 192-193

59 *Ibid*, hal. 239

kemampuan *search*. Pada tiap situs Jughead dan Veronica ada file yang menjelaskan parameter *search* dari program bersangkutan. Veronica sudah lebih lama beredar daripada Jughead dan lebih luas distribusinya[60]

Logika Boolean yang dipakai untuk melakukan pencarian berasal dari hasil pemikiran **George Boole** pada pertengahan abda 19 yang mencakup operator *AND, OR* dan *NOT*. AND digunakan untuk mencari halaman Web yang sekaligus mengandung semua kata-kata yang dimasukkan bai di depan maupun di belakang operator AND. OR digunakan untuk mengakomodasi semua kata atau frasa yang dimasukkan. Jika dalam suatu halaman Web mengandung satu saja dari frasa-frasa yang dimasukkan, maka ia sudah memenuhi syarat untuk ditampilkan. NOT digunakan untuk menyisihkan *frasa* yang tidak dikehendaki, yang berdampingan atau berada dalam suatu halaman Web dengan frasa-frasa lain yang dimasukkan di bagian lain operator NOT.[61]

Alat pencari file dan orang yang lain adalah WAIS atau *Wide Area Information Servers*. WAIS termasuk alat untuk mencari informasi dan memindahkannya. WAIS membantu pengguna dalam mencari dan melihat sumber-sumber di Internet meskipun pengguna tidak tahu tempatnya. WAIS mencari informasi dengan menyebutkan kata atau kalimat dari dokumen yang disimpan dalam pengkalan data yang berhubungan dengan WAIS.[62]

Dari berbagai sisi WAIS adalah alat penjelajah internet yang paling unggul dari semua alat penjelajah internet. Jika pengguna memberitahu WAIS pangkalan data apa yang harus dicari dan kata-kata atau ungkapan yang ingin

---

60 *Ibid*, hal. 117 dan 220

61 FX. Bambang Irawan, *Logika Boolean Efektifkan Pencarian*, Tabloid PCplus No. 12/II/10-16 Januari 2001, hal. 6

62 Randy Raddick dan Elliot King, *op.cit*, hal. 117

pengguna temukan, maka dengan cepat WAIS akan menjelajahi dokumen dalam pangkalan data dan melaporkan jumlah temuan yang disusun menurut jauh dekatnya kata yang pengguna berikan. Setiap temuan diberi nilai 1 hingga 1000. Temuan sempurna bernilai 1000 dan biasanya WAIS memberi nilai 1000 pada temuan yang terbaik.[63]

WAIS mencari informasi dari jaringan, laporan yang disusun dalam indeks menurut topik oleh sukarelawan. Beberapa perusahaan pangkalan jasa, *Dow Jones Information Services* menggunakan program penjelajah WAIS. Pengguna harus membayar untuk jasa tersebut, sedangkan untuk informasi cuma-cuma dari internet, sebagian besar indeks dikerjakan oleh tenaga sukarela.[64]

Finger, Whois, Knowbot dan *Fred* adalah jasa-jasa yang dapat digunakan untuk membantu mencari lokasi alamat-alamat *e-mail* dan informasi lain mengenai orang yang memiliki alamat internet. Finger adalah program yang memungkinkan pengguna memperoleh informasi yang lebih banyak mengenai orang lain jika pengguna tahu domain nama komputer perusahaan jasa yang dilanggani orang itu. Agar Finger dapat berkerja, pengguna harus punya perangkat lunak client Finger pada komputernya dan komputer tujuan harus memiliki server Finger. Finger mempunyai manfaat yang terbatas karena hanya dapat digunakan apabila orang yang akan dihubungi telah pengguna ketahui nama komputer yang menyimpan alamatnya dan komputer itu harus memiliki

---

63 *Ibid*, hal. 261
64 *Ibid*, hal. 261

program server Finger. Lebih sulit lagi banyak lokasi tidak lagi menjalankan program server Finger karena alasan keamanan.[65]

Whois pertama kali dikembangkan untuk mendaftar orang yang bertanggung jawab menjalankan internet dan melakukan penelitian jaringan. Knowbot atau lengkapnya *Knowbot Information Service* atau KIS dapat dipakai oleh pengguna dengan memasukkan satu kata ke KIS. Setelah memasukkan kata tersebut ke KIS maka pengguna dapat mencari seperangkat jasa direktori *white pages* dan melihat-lihat hasilnya dalam format yang seragam. Pengguna dapat menghubungi KIS dengan beberapa cara termasuk dengan *Telnet* dan *e-mail*.[66]

Gopher merupakan alat penjelajah pertama yang menggabungkan proses mencari dan mengambil informasi di Internet. Seperti perangkat lunak lainnya, *Gopher* terdiri atas server dan perangkat lunak client. *Gopher* bekerja dengan perintah berbasis menu. Dengan menggunakan *Gopher* tidak menjadi soal di mana persisnya informasi yang pengguna inginkan itu berada, tidak menjadi soal alat apa yang pengguna perlukan untuk mengambil informasi itu. Pengguna dapat menggunakan alat-alat dari sebuah menu untuk melaksanakan setiap operasi yang bersangkutan.[67]

Gopher adalah hasil karya University of Minnesota yang menyatukan situs-situs komputer yang terpencar-pencar dan alat-alat pencari informasinya berkemampuan tinggi di bawah naungan sistem menu yang sederhana. Pengguna cukup menelpon ke server *Gopher* dan membiarkan *Gopher* menggali *Gopher*space internet hingga tembus ke *Gopher* hole tempat informasi yang

---

65 *Ibid*, hal. 156-157
66 *Ibid*, hal. 117 dan 153.
67 *Ibid*, hal. 118

diperlukan itu berada. *Gopher* mendapat nilai tinggi dari segi mudahnya menggunakan karena menampilkan file teks satu persatu pada layar dan menjalankan perintah menyalin file cukup dengan menekan beberapa tombol saja.[68]

Alat penjelajah yang lain adalah World Wide Web atau WWW.[69] Alat penjelajah ini paling menjanjikan untuk internet saat ini. Teknologi yang digunakan dinamakan *hypertext*.[70] Dengan *hypertext*, kata-kata dalam sebuah dokumen dapat dihubungkan dengan dokumen-dokumen lain. *Link* adalah program *client hypertext* dari keluarga WWW. Program *client Web* dinamakan *browser*.[71]

Bekerja dengan Web mencakup bekerja dengan software *Web Browser* dan *software Web Server*. *Web Browser* sebagai client untuk menginterpretasikan dan melihat informasi Web sedangkan *Web Server* sebagai server untuk menerima informasi yang diminta oleh browser. HTTP (*HyperText Transfer Protocol*) merupakan protokol yang menentukan Web browser dalam meminta atau mengambil suatu dokumen dan menentukan Web server dalam

---

68 *Ibid*, hal. 205

69 Untuk menjelajah dan mencari informasi atas data dengan menggunakan WWW dapat dipakai browser dengan fasilitas search enginenya. Uraian lebih jelas mengenai pemanfaatan fasilitas search engine untuk browser internet explorer dapat dilihat pada tulisan Pandapotan Sianipar, *Mencari Informasi dengan Fasilitas Search IE*, Majalah Internet, Edisi 15 November-15 Desember 2000, hal. 60-59. Baca juga beberapa search engine yang dapat digunakan dalam pencarian di Web dan tip untuk mencari dengan tepat pada rubrik Cakrawala dengan jugul Carilah dengan Search Engine, hal. 24-30

70 *Hypertext* adalah sistem yang dapat menghubungkan informasi melalui *link*. Dengan semakin berkembangnua WWW, istilah *hypertext* kemudian berubah menjadi *Hypermedia*, di mana link penghubung antar informasi bukan lagi berupa teks, tetapi bisa berupa file multimedia, seperti gambar, suara atau video. Hypermedia merupakan perluasan dari hypertext, sebuah istilah untuk inforasi atau narasi yang kait mengait. Produk multimedia yang mencakup televisi interaktif dan komputer bisa berfungsi sebagai video. Nicholas Negroponte, *op.cit.*, hal. 76-77. Lihat juga Tim DSM STIKOM Surabaya, *Pengantar HTML*, Infokomputer, Edisi Internet, Vol. 1 No. 6 Edisi 15 Juli-15 Agustus 1997, hal. 42.

71 Randy Raddick, *op.cit*, hal. 118-119

menyediakan dokumen yang diminta oleh Web browser. HTTP digunakan untuk menjelajahi Web yang berhubungan dengan banyak protokol lain. Format data yang dipakai untuk membuat dokumen *hypertext* dinamakan *HyperText Markup Language* (HTML). Dokumen HTML disebut *Mark Language* karena berisi tanda-tanda tertentu yang digunakan untuk menentukan tampilan suatu teks dan tingkat kepentingan dari teks tersebut dalam suatu dokumen yang dapat dilihat oleh semua orang pada komputer apapun dengan browser apapun. [72]

Selain program lunak aplikasi yang disebut di atas, ada juga program aplikasi yang bersifat interaktif. Program ini memungkinkan pengguna bercakap-cakap dengan orang lain melalui jaringan internet. Program tersebut antara lain adalah Newsgroup, Mailing List dan Internet Relay Chat. Newsgroup dapat diibaratkan sebagai sebuah majalah dinding besar yang bisa diisi dan dibaca oleh siapa saja melalui surat elektronik.[73] Dari segi struktur, newsgroup memiliki beberapa kelebihan dibandingkan dengan kelompok diskusi yang dikelola melalui *litserv* atau mailing list, karena berita tidak dikirimkan ke komputer pribadi tetapi berada dalam server, maka bila membaca berita-berita newsgroup, kotak *e-mail* tidak dipenuhi berita-berita newsgroup. Di samping kelebihan itu, newsgroup juga memiliki kelemahan berkaitan dengan mutu informasi yang disampaikan. Mutu informasi yang disampaikan ada yang baik

---

[72] *Ibid.* Untuk membuat sebuah halaman web tidak diperlukan software tertentu, yang diperlukan hanyalah sebuah teks editor serta pengetahuan tentang HTML itu sendiri. Bahasa HTML adalah sekumpulan aturan tentang bagaimana sebuah dokumen HTML disusun dan aturan-aturan itu disebut *tag*.Bagaimana membuat halaman web dengan HTML dengan aturan tagnya, dapat dipelajari secara lebih mendetail dalam Samuel Prakoso, *Mengenal HTML*, Buletin Jendela Informatika Vol. 2 No. 1, 2001, hal. 42-42 pada rubrik Jendela Tutorial atau buku dan majalah lain yang menyajikan informasi serupa.

[73] Arnahedi Mazhar, *op.cit*, hal. 11

sekali dan ada pula yang keliru. Terkadang sulit membedakan mana yang benar dan mana yang salah.[74]

Mailing list alias *milis* dapat diibaratkan sebagai kumpulan surat terbuka elektronik yang dikirimkan langsung hanya kepada anggota-anggotanya,[75] ada pula yang mengibaratkan sebagai pengikat psikologis virtual bagi pecinta *e-mail*.[76] Konsep kerja *mailing list* pada dasarnya sangat sederhana. Seorang pengguna cukup mengirimkan *e-mail* ke satu alamat *e-mail* yang kemudian disebarkan ke semua member mailing list yang tergabung atau berlangganan ke alamat *e-mail* tersebut. Dari sini terlihat bahwa mailing list merupakan media yang lebih bersifat interaktif dan pro aktif dibandingkan web yang biasa ada di internet.[77]

Internet Relay Chat (IRC) atau chat dapat diibaratkan sebagai ruang santai yang di dalamnya banyak orang di seluruh pelosok dunia dapat mengobrol secara tertulis tanpa bertatap muka pada waktu yang bersamaan.[78] IRC pertama kali ditulis oleh **Jarkko Oikarinen** di Finlandia pada tahun 1988. IRC dapat digunakan untuk bercakap-cakap dengan banyak orang sekaligus, artinya orang berkumpul dalam saluran (*channel*) untuk bercakap-cakap, dalam kelompok,

---

74 Randy Raddick dan Elliot King, *op.cit*, hal. 276

75 Armahedi Mazhar, *op.cit.*

76 Yus Dwi Handoko, *Membuat Mailing List di eGroups*, dalam majalah Internet, Edisi 15 November - 15 Desember 2000, hal. 60-62

77 Konsekuensi yang harus ditempuh oleh orang atau perusahaan yang akan menggunakan mailing list adalah harus dapat berinteraksi atau merespon secara cepat menggunakan *e-mail* karena semua pengguna *e-mail* di internet berharap agar respon dapat dilakukan secara cepat. Mailing list merupakan bentuk dasar dari diskusi secara elektronik yang berbasis elektronik mail. Kendati dibentuk jauh sebelum web menjadi populer dan memenuhi traffic internet seperti saat ini, mailing list merupakan sarana yang sangat ampuh - lebih ampuh daripada web yang sifatnya lebih pasif. Onno W. Purbo, *Diskusi Melalui Mailing List Di Internet*, Infokomputer Edisi Internet, Vol. I No. 4, Mei-Juni 1997 hal. 19. Yus Dwi Handoko, *op.cit.* Di samping itu mailing list juga menyediakan *one-stop shopping* untuk informasi yang sulit dicari. Mailing list merupakan cara yang tepat untuk mendapatkan informasi secara cepat yang susah dicari sendiri. Lihat juga Yus Dwi Handoko mengeai cara kerja mailing list. *Mailing List: One-Stop Shopping Untuk Masalah Anda*, dalam Majalah Infokomputer Vol. XI No. 5 Mei 1997, hal. 28-32

78 Armahedi Mazhar, *op.cit.*, hal. 11

secara terbuka atau pribadi. IRC muncul sebagai saluran komunikasi pintu belakang yang menarik untuk meliput suatu kejadian penting bagi wartawan.[79]

Kemajuan yang dicapai dalam bidang teknologi informasi dengan ditemukannya *video camera* membuat *chatting* sekarang menjadi semakin menarik. Tetapi hal ini belum sepenuhnya dapat dinikmati oleh pengguna apabila pengguna menggunakan koneksi *dial up* dengan memanfaatkan jaringan telepon karena sering terjadi *disconnect*, terputus-putus dan lambat.[80] Dengan teknologi *broadband* tentunya kendala tersebut dapat teratasi. Jika kendala itu teratasi maka *web camera* ini selain untuk *chatting* juga dapat dimanfaatkan untuk membuat video klip mini atau membuat situs pribadi.

Berkembangnya *web camera* akan membuat komunikasi lebih interaktif apalagi dengan adanya *Voice over Internet Protocol* (VoIP).[81] VoIP merupakan jasa telekomunikasi yang memungkinkan seseorang melakukan percakapan langsung (baik untuk SLI maupun) atau menghubungkan pengguna telepon suara melalui internet dengan biaya yang sangat murah karena dihitung dengan pulsa lokal.[82] Jika *chatting* memungkinkan seseorang melakukan

---

79 Randy Raddick dan Elliot King, *op.cit*, hal, 301

80 Silvester Sila Wedjo, *Video Camera: Bikin Chatting Tambah Seru*, Tabloid PCplus No. 16/II/14-20 Februari 2001, hal. 21

81 Perkembangan VoIP yang pesat di Indonesia saat ini disebabkan karena dibukanya kompetisi Internet Service Provider yang saat ini mencapai 139 perusahaan dan VoIP merupakan salah satu pengembangan internet yang berkembang sangat pesat. Di samping itu teknologi VoIP sulit dibendung karena peminatnya sangat banyak baik yang mengajukan secara legal permohonan untuk memasang VoIP maupun yang menggunakan VoIP illegal. Kecenderungan ini menyebabkan Direktorat Jenderal Pos dan Telekomunikasi berusaha untuk membuat regulasi dan kebijakan di bidang VoIP di samping bidang-bidang yang berkaitan dengan internet lainnya. Ismail Ahmad, *Regulasi Voice over Internet Protocol*, Makalah pada Seminar Teknologi 2k dengan tema Voice over Internet Protocol, dalam rangka Dies Natalis XVII Teknik Elektro UNDIP, 14 Desember 2000 di Ghradika Bakti Praja, Semarang, hal. 4

82 Murahnya biaya menggunakan VoIP untuk percakapan tidak hanya ditentukan oleh perhitungan pulsa semata, tetapi juga oleh teknologi yang dipakainya, jika internet menggunakan packet-switched network maka VoIP dengan Public Switch Telephony Network (PSTN) digunakan melalui circuit-switched network. Sebab-sebab kemurahan yang lain secara teknis dapat dibaca lebih jelas dalam makalah Arya Satriananta, *Internet Telephony, A Broader Business Perspective of Delivering Telephony Service over Internet*, Makalah pada Seminar Teknologi 2k dengan tema Voice over Internet Protocol, dalam rangka Dies Natalis XVII Teknik Elektro UNDIP, 14 Desember 2000 di Ghradika Bakti Praja, Semarang, hal. 5-8

> Information and communication technology has invaded all domains of our society: at work, at home and in public places. In modern culture is profoundly mediated. Current innovations in computers and telecommunication made new kinds of social interaction and cultural transmission possible across previously impossible distances. There is little doubt that these rapid advances in modern telecommunication and computers are changing the way we live our lives, but the direction of change is still uncertain[86]

Teknologi komunikasi yang berkembang selama ini seperti telepon, sebenarnya dapat menolong manusia untuk mendorong dalam memelihara hubungan yang baik dan memperpendek jarak, demikian juga dengan televisi. Tetapi seperti dikatakan oleh **John Perry Barlow**, dalam televisi memang ada keterhubungan yang berlangsung, namun secara keseluruhan pemirsa televisi mendapatkan ketakterhubungan yang menyamar dalam bentuk keterhubungan dalam segala bentuknya yang tersembunyi.[87]

Penggabungan teknologi telekomunikasi dan komputer (internet) menjadi komunikasi berbasis komputer mempunyai konsekuensi lebih besar daripada pemanfaatan telepon dan televisi secara tersendiri, seperti yang dikatakan oleh **D. Beckers**:

> But the merge of telecommunication and computers, the computer mediated communication (CMC) might have an even bigger consequences than the telephone and the television, because of its unique characteristics. In the first place the ease to generate and distribute data are unknown to any earlier technique based on this data can be generated, for example searching-mechanism. Second, CMC is not limited to only text, but also transport pictures audio and video. Third, CMC is the first many-to-many medium, For example the telephone can only be used by two percent at a time (one-to-one) and a

---

86 D. Beckers, *Research on Virtual Communities: An Empirical Approach*, dapat dijumpai di http://www.swi.psy.uva.nl/usr/beckers/publication/seattle.html Bandingkan dengan pendapat M. Ethan Katsh yang menyatakan I have argued that the new media are a significant cultural and legal phenomenon not because they enable us to perform informational tasks faster than before but because they change how we interact with distant information and distant people. M. Ethan Katsh, *Cybertime, Cyberspace and Cyberlaw*, Journal of Online Law, June 1995.

87 John Perry Barlow dalam percakapannya dengan Jeff Zaleski. Jeff Zaleski, *op.cit.*, hal. 66-67

> newspapthe send information from one source to many (one-to-many). Last, CMC can be used both synchronies (for example for a telephone call the participants have to use the telephone at the same time) as a asynchronous (for example a letter, that is written beforehand and is read later)[88]

Computer Mediated Communication (CMC) atau komunikasi berbasis komputer, meliputi jaringan komputer, elektronik mail, *Electronic Bulletin Board Service* (BBS) dan pertemuan dengan menggunakan komputer. Istilah informal yang dipakai oleh **Howard Rheingold** untuk menyebutkan interkoneksi jaringan komputer yang menggunakan teknologi CMC untuk menghubungkan orang-orang di seluruh dunia untuk diskusi publik dinamakan *Net.*

Komunikasi berbasis komputer mempunyai keuntungan tersendiri, diantaranya adalah berkurangnya pola diskriminisasi komunikasi yang didasarkan pada keadaan fisik dan sosial seperti gender, ras, status sosial ekonomi, keadaan fisik dan sebagainya. sebagaimana diungkapkan oleh **Mark Poster**, "*As a result, CMC destabilizes existing hierarchies in relationships and rehierarchize communication patterns according to criteria that were previously irrelevant*".[89] CMC juga mempertinggi interaksi seseorang dengan orang lain yang tidak terbatas pada tempat, waktu, luas bidang yang diperbincangkan atau dengan kata lain interaksi yang bersifat multidimensional dan serta tidak lagi terganggu oleh batas-batas konvensional dalam berinteraksi.

CMC diyakini mempunyai pengaruh yang sangat besar dalam hubungan sosial, partisipasi masyarakat dalam demokrasi, pendayagunaan

---

88 D. Beckers, *op.cit*

89 Mark Poster, sebagaimana dikutip oleh Kumiko Aoki, *Virtual Communities in Japan*, Paper pada The Pacific Telecommunication Council 1994 Conference, dapat dijumpai di http://metalab.unc.edu/pub/academic/communications/papers/Virtual-Communities-in-Japan dan http:// www.vcn.bc.ca/sig/comm-nets/aoki.txt

sekedar hubungan melalui internet. Ketika kita sedang menelpon atau membaca buku, ada ruang yang muncul (yang juga dinamakan *cyberspace* oleh **Barlow**), tetapi ruang yang tercipta itu tidak mungkin untuk berinteraksi secara *real-time*.[92]

Dengan merujuk kepada hal tersebut maka *cyberspace* sebetulnya sudah ada ketika **Alexander'Graham Bell** menemukan telepon dan **Gutenberg** merintis pencetakan buku. Meski demikian waktu itu orang tidak menyebut ruang yang tercipta sebagai *cyberspace*. Istilah *cyberspace* itu sendiri muncul pertama kali dari novel **William Gibson** berjudul *Neuromancer* yang diterbitkan pada tahun 1984. Waktu itu **Gibson** mendefinisikan *cyberspace* sebagai

> "A consensual hallucination experienced daily billions of legitimate operators, in every nation..... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding."[93]

Pada waktu itu istilah *cyberspace* oleh **Gibson** belum ditujukan pada interaksi yang terjadi melalui jaringan komputer. Istilah *cyberspace* yang benar-benar ditujukan pada interaksi yang terjadi di internet adalah pada tahun 1990 ketika **John Perry Barlow** untuk pertama kalinya mengaplikasikan istilah *cyberspace* untuk dunia yang terhubung atau online ke internet.[94]

---

92 *Cyberspace* menurut John Perry Barlow adalah ruang yang muncul ketika anda sedang menelpon. *Cyberspace* adalah setiap ruang informasi, tetapi ia adalah ruang interaksi interaktif yang diciptakan oleh media yang begitu padat sehingga di sana ada kesadaran tentang kehadiran orang lain. Bandingkan dengan definisi yang diberikan oleh Wired Style: Principle of English Usage in the Digital Age dan dari Que's Computer and Internet Dictionary pada Jeff Zaleski, *loc.cit*, hal. 53-54 dan definisi yang diberikan oleh Yasraf dalam Mark Slouka, *op.cit.*, hal. 19.

93 William Gibson, *Neuromancer*, New York: Ace, 1984, hal. 51. Bandingkan dengan definisi-definisi lain yang terdapat dalam Mark Slouka, *op.cit.* hal. 14. Bandingkan pula dengan Jeff Zaleski, *op.cit.*, hal 54

94 *The Growth and Development of Cyberspace Law in the United States: Highlights of the Past Decade*, The UCLA Online Institute for *Cyberspace* Law dan Policy. Lihat juga percakapan antara Jeff Zaleski dan John Perry Barlow dalam Jeff Zaleski, op.cit., hal 53

masyarakat dan bentuk-bentuk tantangan lain. Hal ini terungkap dari pendapat yang dikemukakan oleh **Peter Kollock** dan **Marc Smith** sebagai berikut :

> Many claim that this new form of social interaction encourages wider participation, greater candor, and an emphasis on merit over status. In short, the belief is that social hierarchies are dissolved and that flatter, more egalitarian social organizations emerge. Networked communications, it is argued, will usher in a renewed era of democratic participation and revitalized community. But as with earlier technologies that promised freedom and power, the central problems of social relationship remain, although in new and possibly more challenging forms.[90]

Meskipun demikian, ada pertanyaan mendasar mengenai CMC ini dalam ilmu sosial mengenai permasalahan kerjasama (*cooperation*). Bagaimana mungkin sekelompok orang yang tidak berada di satu tempat yang bersamaan dapat mengatur untuk menciptakan dan memelihara hubungan kerjasama. Pertanyaan ini menjadi perhatian yang serius setidak-tidaknya bagi **Peter Kollock** dan **Marc Smith** yang mengemukakan pendapatnya tentang permasalahan tersebut.

> The character and qualities of this problem are different when groups use computer-mediated communication to interact, but the differences do not guarantee a uniformly positive effect or resolve many of the long standing problems of cooperation. Indeed, we will show that there is a double edge to computer mediated interaction: many of its central qualities make it easier both to cooperate and to behave selfishly. Thus, computer-mediated interaction raises political, practical, and sociological problems in new ways and with new stakes.[91]

Pengertian *cyberspace* tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet. Setidak-tidaknya dengan memperhatikan definisi tentang *cyberspace* dari **John Perry Barlow**, *cyberspace* lebih luas dari

---

90 Peter Kollock dan Marc Smith, *Managing the Virtual Commons: Cooperation and Conflict in Computer Communities*, dalam *Computer-Mediated Communication: Linguistic, Social, and Cross-Cultural Perpective*, (page 109-128) editor Susan Herring. Versi Electronik dapat dijumpai di http://www.sscnet.ucla.edu/soc/faculty/kollock/papers/vcommons.html

91 Peter Kollock dan Marc Smith, *ibid.*

John Suler menganggap bahwa *cyberspace* adalah ruang psikologis, dan sebagai ruang psikologis, keberadaannya tidaklah tergantung pada batas-batas konvensional mengenai keberadaan benda berwujud. Bedanya dengan benda yang wujudnya berada dalam dunia nyata, *cyberspace* sebagai hasil teknologi tidak berada dalam dunia nyata tetapi ia betul-betul ada. **John Suler** dalam artikelnya *The Psychology of Cyberspace, Overview and Guided Tour* mengungkapkan

> "*Cyberspace* is psychological space. The psychological study of *cyberspace* is as broad as the field of psychology itself. Anyone who has taken an introductory psychology course known how vast that terrain is. Cognitive psychology, personality theory, social psychology, development psychology, clinical psychology - all are relevant.[95]

Terlepas dari permasalahan istilah *cyberspace*, yang perlu diperhatikan sekarang adalah bahwa masyarakat global sekarang telah memasuki dunia baru yang di dalamnya dapat berbuat apapun seperti yang dapat dilakukan di dunia nyata, dengan tingkat pengalaman yang sama yaitu di dalam jagat raya *cyberspace*. *Cyberspace* telah berkembang dan meluas dan secara fundamental telah menggasak definisi lama tentang ruang fisik, identitas dan komunitas.[96]

Hubungan ekonomi, komunikasi dan koordinasi di *cyberspace* berbeda dengan ketika orang bertemu secara tatap muka (*face to face*). Dalam *cyberspace* kita dapat melakukan diskusi mengenai berbagai hal, bercanda dan hiburan. *Cyberspace* menjadi media untuk berbagai hal sebagaimana dikatakan oleh **Licklider** dan **Harasim**.

---

95 John Suler, The Psychological of *Cyberspace*, Overview and Guided Tour, September 1999, versi elektronik dapat dijumpai di http://www.rider.edu/users/suler/psycyber/psycyber.html

96 Mark Slouka, op.cit., hal. 13 dan 55

> Using network interaction media like e-mail, chat, and conferencing systems like the Usenet, people have formed thousand of groups to discuss a range of topics, play games, entertain one another, and even work on a range of complex collective project. These are not only communication media - they are group media, sustaining and supporting many to many interactions.[97]

Dalam menangkap realitas, manusia dibatasi oleh ruang dan waktu. Artinya pada saat yang sama, orang tidak mungkin berada di dua atau lebih tempat yang berbeda. *Cyberspace* telah melingkupi berbagai sisi dari kehidupan modern, dan memungkinkan hubungan yang terjadi tanpa mempermasalahkan jarak, waktu dan tempat/ruang. Konsep mengenai jarak (*distance*), waktu (*time*) dan ruang (*space*) merupakan konsep dalam instutusi sosial yang penting.

Internet yang menghadirkan *cyberspace* mengubah secara mendasar konsep tersebut, artinya jarak, waktu dan ruang tidak lagi menjadi halangan untuk berkomunikasi sebagaimana dikatakan oleh **Harold Innis**, seorang ahli ekonomi Kanada lebih dari 40 tahun yang lalu

> Harold Innis suggested that the introduction of new medium of communication sets in motion deep-rooted change in important societal institutions by influencing orientations about time and space. Writing more than a decade before "the medium is the message became part of popular culture, Innis asserted than "the materials on which words were written down have often counted for more than the words themselves."[98]

---

97 Licklider (1978) dan Harasim (1993) dalam Peter Kollock dan Marc Smith, *Communities in Cyberspace* (ed), London: Routledge, 1999, versi electronik dapat dijumpai di http://www.sscnet.ucla.edu/soc/faculty/kollock/papers/communities_01.html

98 Harold Innis, sebagaimana dikutip oleh M. Ethan Katsh, *op.cit.* Bandingkan dengan hukum yang bekerjanya juga dibatasi oleh waktu dan ruang sebagaimana pengamatan dari Hakim Brandeis, The law is limited by time and space." More than this, the law might be said to have a "sense of place" or be " of a place" in that there are informational places that are central to process and operation of law. Bandingkan pula dengan pendapat Howard Rheingold yang mengatakan Computer conferencing emerged, also somewhat unexpectedly, as a tool for using the communication capacities of the networks to build social relationships across barriers of space and time. Howard Rheingold, *Virtual Reality*, Mandarin, 1991, versi electronic dapat dijumpai di http://www.rheingold.com/vc/book/intro.html

Berkembangnya pemanfaatan *cyberspace* untuk berbagai keperluan dalam kehidupan manusia tidak lepas dari apa yang dinamakan sebagai revolusi teknologi informasi. Banyak istilah yang digunakan orang untuk menandai perkembangan internet ini, seperti revolusi digital, revolusi informasi, abad informasi dan sebagainya. Tetapi untuk memahami hal tersebut tentunya perlu perhatian yang lebih mendalam.

Mark Slouka memandang bahwa untuk memahami revolusi digital, maka yang harus diketahui ada dua hal. *Pertama*, komputer (yang bukan alat sekedar pengolah informasi, tetapi sedang berkembang menjadi mesin peniru canggih) memiliki kemampuan yang kini meningkat untuk meniru aspek-aspek tertentu kehidupan kita. *Kedua*, sejumlah besar orang jenius dan berpengaruh percaya bahwa komputer harus dan akhirnya akan mengusur dunia asli yang telah berhasil diimitasikan itu.[99]

Cyberspace yang menghadirkan realitas virtual juga dianggap sebagai sebuah *revolusi realitas*. *Cyberspace* menjadi tempat bagi setiap orang untuk menemukan demokrasi, tempat orang mencurahkan pendapatnya dan bebas untuk berbicara apa saja karena *cyberspace* adalah ruang yang bebas. Anggapan demikian tidak terlepas dari dominasi media cetak dan elektronik yang sering memanipulasi peristiwa dan data yang diungkapkan lewat berita-beritanya.[100]

---

[99] Para cyberis berusaha meyakinkan visi ini dengan semangat evangelisnya baik melalui buku dan artikel, ruang kelas, pameran komputer, simposium dan lain sebagainya. Jadi perbesarlah bandwidth, kata para cyberis menanggapi hal tersebut. Mark Slouka, *op.cit*, hal, 61-62.

[100] Dalam konteks ini adalah dominasi yang dilakukan oleh Paramount Communication and Time Warner dan Rupert Murdoch's News Corporation, yang menyebabkan orang melihat internet sebagai ruang yang bebas untuk mengkritik dan berbicara. Jon Wiener, *Static in Cyberspace*, The Nation Magazine, June 13, 1994, dapat dijumpai di http://www.igc.apc.org/

Cyberspace menjadi ruang yang bebas untuk melontarkan kritik dan kebebasan berpendapat, kebebasan dari aturan main yang ditentukan oleh media massa. *It's the most universal and indispensable network on the planet. The internet is anarchic but also democratic*, kata **Jon Weiner** seorang *Free Speech* di Internet. Internet atau disebut juga dengan berbagai istilah seperti *Net, Online* dan *Web,* merupakan ruang yang bebas karena tidak ada kontrol dari manapun, tidak ada pusatnya, sehingga ketika pemerintah suatu negara hendak membatasi dengan cara melakukan sensor, mendapat tanggapan yang cukup serius dari para *cyberis* dan *teknoevangelis.* Di antaranya adalah **John Perry Barlow** yang mengeluarkan *Declaration of the Independent of Cyberspace* sebagai bentuk protesnya. Berikut dokumen *declaration* tersebut secara lengkap seperti yang dipublikasikan oleh **Barlow** dalam situsnya.

A DECLARATION OF THE INDEPENDEN OF *CYBERSPACE*[101]

> Government of the Industrial World, you weary giants of flesh and steel, I come from *Cyberspace*, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
> We have no elected government, nor are likely to have one, so I address you with no greater authority than that with which liberty itself always speak. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we true reason to fear.
> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. *Cyberspace* does not lie within your borders. Do not think that you can build it, as thought it was a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.
> You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our

[101] Dikutip sesuai dengan aslinya, dapat dijumpai di http://www.eff.org/~barlow.

culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concept of property, expression, identity, movement, and context do not apply to us. They are based on matter. There is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust you bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expression of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokers from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of *Cyberspace*. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claims to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In

> our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.
> These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.
> We will create a civilization of the Mind in *Cyberspace*. May it be more humane and fair than the world your governments have made before.
> John Perry Barlow, Cognitive Dissident
> Co-Founder, Electronic Frontier Foundation
> Davos, Switzerland
> February 8, 1996.

Apa yang dikemukakan oleh **Barlow** merupakan manifestasi dari rasa kekesalannya atas pembatasan yang dilakukan oleh negara (khusunya Amerika Serikat di mana **Barlow** secara fisik tinggal di sana). Bagi kalangan *cyberis*, ada pepatah yang mengatakan ***informasi ingin bebas***. Pepatah inilah yang mengilhami para *cyberis* untuk menentang pembatasan-pembatasan yang dilakukan oleh pemerintah suatu negara.

Cyberspace sudah menjadi tempat yang sangat luas. Ia ibarat lautan.[102] Setiap orang atau mahluk apapun dapat mengarungi lautan itu, seperti virus komputer. *A Declaration of the Independence of Cyberspace* memang berasal dari **John Perry Barlow**, tetapi begitu masuk ke *cyberspace*, ide tersebut mengambil bentuk hidupnya sendiri dan terus menjelajahi *cyberspace* tanpa campur tangan **Barlow** lagi.[103]

A Declaration of the Independence of Cyberspace yang dikemukakan oleh Barlow lebih ditekankan kepada kebebasan ruang saja yaitu kebebasan di

---

[102] Jeff Zaleski, *op.cit.*, hal. 161
[103] *Ibid*, hal. 60

cyberspace sedangkan kebebasan para penghuninya yang disebut *Netizens* tidak menjadi perhatian pokok. Berkaitan dengan kebebasan *netizens* dalam berkreasi dan berinteraksi di *cyberspace*, mereka mengajukan deklarasi mengenai hak-hak mereka seperti yang diungkapkan oleh **Ronda Hauben** dalam karyanya *Netizens: On The History and Impact of the Net.* Berikut petikan usulan deklarasi tersebut

> *THE DECLARATION OF THE RIGHTS OF NETIZENS*
>
> In recognition that the net represents a revolution in human communications that was built by a cooperative non-commercial process, the following Declaration of the Rights of the Netizen is presented for Netizen comment
> As Netizens are those who take responsibility and care for the Net, the following are proposed to be their rights:
> - Universal access at no or low cost
> - Freedom of Electronic Expression to promote the exchange of knowledge without fear of reprisal
> - Uncensored Expression
> - Access to Broad Distribution
> - Universal and Equal access to knowledge and information
> - Consideration of one's ideas on their merits
> - No limitation to access to read, to post and to otherwise contribute
> - Equal quality of connection
> - Equal time of connection
> - No Official Spokesperson
> - Uphold the public grassroots purpose and participation
> - Volunteer Contribution - no personal profit from the contribution freely given by others
> - Protection of the public purpose from those who would use it for their private and money making purposes.
>
> The Net is not a Service, it is a Right. It is only valuable when it is collective and universal. Volunteer effort protects the intellectual and technological common-wealth that is being created. DO NOT UNDERESTIMATE THE POWER OF THE NET and NETIZENS.[104]

---

[104] Ronda Hauben, *Netizens: On The History and Impact of The Net*, pada bagian ke 13 *mengenai Proposed Declaration of the Rights of Netizens*, versi elektronik dapat dijumpai di http://www.columbia.edu/~rh120/ch_d13_rights.html.

Deklarasi ini dibuat berdasarkan pada *Request for Comment* (RFC) tahun 1969, *Thomas Paine, Declaration of Independence (1776), Declaration of Human Rights of Man and of Citizen (1789), NSF Acceptable Use Policy, Jean Jacques Rousseau* dan penderitaan demokrasi yang terjadi di dunia ini. Deklarasi ini belum final, artinya mereka-mereka yang menjadi penghuni *cyberspace* dapat mengirimkan pendapat, ide, gagasan dan kontribusi lain agar deklarasi ini menjadi lebih baik dan dapat melindungi para netizens dari tindakan pihak-pihak yang mengekang atau mencabut hak-hak *netizen* dalam berkreasi dan beraktivitas di *cyberspace*.

Realitas sosial budaya yang ada pada *cyberspace* merupakan tandingan dari realitas sosial budaya yang ada dan menghasilkan batas antara keduanya pada akhirnya menjadi kabur. *Cyberspace* sebagai satu bentuk jaringan komunikasi dan interaksi global telah menawarkan bentuk komunitas tersendiri, yaitu komunitas virtual (*virtual community*).[105] **Menurut Howard Rheingold,** *virtual community* adalah *social aggregations that emerge from the Net when enough people carry on those public discussion long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace.*[106] Hal senada secara panjang lebar juga diungkapkan **oleh John Suler** sebagai berikut

> Its social climate partly is shaped by is demographics. As world structured by machines rather than the physical environment, it also is a space with some rather unique psychological features-such as reduced or altered sensory experience, the opportunity for identity flexibility and anonymity, the equalization of social status, the transcending of spatial boundaries, the stretching and condensation of time, the ability to access numerous relationships, and the capacity to record permanent records of one's experiences... to name a few. It is a world with its

---

[105] Yasraf Amir Piliang dalam pengatar buku Mark Slouka, *loc.cit*, hal. 19
[106] Howard Rheingold, *op.cit.*

> own language. As a virtual reality, it can offer us true-to-life experiences as well as highly imaginative scenarios.[107]

Dalam *cyberspace* ada yang dinamakan WELL (*Whole Earth 'Lectronic Link*), sebuah tempat yang memungkinkan orang-orang dari seluruh dunia berbicara atau bercakap-cakap satu sama lain dan bertukar atau berkirim surat elektronim (*e-mail*). Dari sinilah muncul ide tentang munculnya masyarakat (*community*), di mana setiap orang di seluruh dunia dapat menjadi anggotanya asalkan menghubungkan komputer pribadinya (atau komputer di kantornya) melalui telepon dan modem ke jaringan komputer global. Pengalaman bergabung dengan masyarakat digital dapat dirasakan sebagaimana pengalaman yang dikemukakan oleh **Howard Rheingold**

> The idea community accessible only via my computer screen sounded cold to me at first, but I learned quickly that people can feel passionately about e-mail and computer conferences. I've become one of them. I care about these people I met through my computer, and I care deeply about the future of the medium that enables us to assemble.[108]

Gagasan tentang komunitas virtual sudah menjadi pandangan umum karena komunitas virtual itu memang betul-betul ada. *Cyberspace* telah saling menghubungkan banyak orang namun hal ini tidak menjamin komunitas karena keterhubungan yang dibuat oleh *cyberspace* sering bersifat satu arah atau dengan kata lain aliran informasi masih bersifat siaran. Meski demikian dengan adanya fasilitas internet yang bersifat interaktif (secara online) orang bisa bertukar informasi dan di sini ada komunitas dalam pengertian yang lebih luas[109]

---

107 John Suler, *op.cit.*

108 Howard Rheingold, *ibid.* Baca juga mengenai komunitas on-line dalam Baca lebih lengkap mengenai komunitas digital atau online ini pada Anne Beamish, *Communities On-line: Community-Based Computer Networks*, Thesis at the Massachesetts Institute of Technology, February 1995 lihat di http://loohooloo.mit.edu/4.207/anneb/ thesis/toc.html

109 Jeff Zaleski, op.cit., hal. 273

Orang-orang dalam dunia virtual tidak menghadirkan fisiknya untuk berkomunikasi dengan orang lain melainkan menggunakan kata-kata dalam layar komputer. Dengan berkembangnya VoIP (*Voice of Internet Protocol*) dan *Web camera* memungkinkan hadirnya suara dan wajah dalam berkomunikasi sehingga komunikasi yang terjadi berupa *computer conference*. Dalam *virtual community* dapat berkomunikasi dengan identitas apa saja karena identitas asli dalam dunia nyata (*real life*) dapat ditinggalkan di belakangnya seperti dikatakan oleh **Howard Rheingold,** *"People in virtual communities do just about everything people do in real life, but we leave our bodies behind".*[110] Para penghuni *cyberspace* tidak hanya meninggalkan tubuhnya dan berkelana dalam alam maya itu, tetapi ia dapat juga mengganti identitasnya (dari laki-laki menjadi perempuan atau sebaliknya), pekerjaannya, statusnya dan lainnya.

Dalam komunitas virtual perbedaan-perbedaan yang ada di dunia nyata menjadi tidak penting. Gender, ras dan usia menjadi tidak penting dalam interaksi secara online.[111] Dengan mendasarkan pada pendapat **Jodi O'Brien, Kollock** dan **Smith** mengemukakan

> There are no limitations to how one might describe oneself in *cyberspace*. Yet the gender descriptions one encounters on the Internet show far less variation and imagination than occurs in face-to-face interaction. People recreate themselves as stereotypical ideals, and O'Brien points out that this "hyper-gendering" is especially prevalent among those who attempt to "cross-dress," (i.e. males presenting themselves as females). The implication is that a world without

---

110 Howard Rheingold, *op.cit.*

111 Hal itu dikemukakan oleh Kollock dan Smith. Secara lebih lengkap ia mengemukakan bahwa *the most optimistic proponents of the Internet have argued that gender, race and age become unimportant in online interaction. At the very least, many assumse that the absence of these markers willprovide the opportunity to explore and invent alternate identities.* Peter Kollock dan Marc Smith, *Communities in Cyberspace*, *op.cit.*

constraints has led to greater homogeneity rather than new forms of identity.[112]

Realitas yang dihadapi dari komunitas virtual adalah realitas virtual (*virtual reality*). Istilah realitas virtual pertama kali diperkenalkan oleh **Jaron Lanier**, seorang peramal ulung di bidang *cyberspace*. Pada usia 30-an, ia memperoleh ketenaran atas di seluruh dunia pada akhir 1980-an atas penemuannya berupa komponen *virtual reality* dasar seperti sarung tangan dan jaringan *virtual reality*.[113]

Realitas virtual bukanlah sebentuk representasi realitas dalam pengertiannya yang biasa. Realitas virtual sebaliknya adalah sebentuk simulasi realitas seperti dikatakan oleh **Jean Baudrillard** dalam *Simulations* bahwa simulasi realitas adalah penciptaan model-model kenyataan yang tanpa asal-usul atau realitas *hyperreal*. Sedangkan **Steve Aukstakalnis** dan **David Blatner** menjelaskan realitas virtual sebagai cara manusia untuk memvisualisasikan, memanipulasi dan berinteraksi dengan komputer dan data yang sangat kompleks.[114]

Cyberspace dengan realitas virtualnya menawarkan kepada manusia untuk hidup di dalam dunia alternatif, dunia yang melampaui realitas yang ada. Ia juga menawarkan berbagai kemudahan, keindahan dan kenikmatan. Tetapi

---

112 Jodi O'Brien mengemukakan pendapatnya dalam buku *Writing in the Body: Gender (Re) Production in Online Interaction*. Secara lebih lengkap ia mengemukakan Gender is such central feature for organizing interpersonal relations that persons go to great pains to reproduce gender in online interaction. Are you male or female? is such a commonly asked question that it was long ago abbreviated to "RUMorF?" Significantly, no such abbreviations are in widespread use for questions concerning age, height, weight, socio-economic status, etc. Gender is the one characteristic of our embodied lives that is a central feature in interaction throughout the Internet. Peter Kollock dan Marc Smith, *ibid.*

113 Jeff Zaleski, *op.cit.*, hal. 159

114 Yasraf Amir Piliang dalam Mark Slouka, *op.cit.*, hal. 16

yang perlu diwaspadai adalah bahwa di samping tawaran yang menggiurkan itu, *cyberspace* juga menawarkan keburukan-keburukan.

Setidak-tidaknya ada tiga pandangan yang berbeda dalam melihat dunia realitas virtual tersebut. [115] *Pertama*, orang-orang yang melihat realitas virtual dengan pandangan yang optimistis, positif, *affirmative* (**Timothy Leary, Rheingold**). Keoptimisan mereka terungkap dalam pendapat yang dikemukakan oleh **Howard Rheingold**

> Because of its potential to change us as humans, as communities, as democracies, we need to try to understand the nature of CMC, *cyberspace*, and virtual communities in every important context-politically, economically, socially, cognitively. ... I care about what happens in *cyberspace*, and to our freedoms in *cyberspace*, because I dwell there part of the time.[116]

Termasuk dalam golongan yang pertama adalah Wakil Presiden Amerika Serikat (1993-2001) **Al Gore** yang menggambarkan visinya dengan mengatakan "*Our new ways of communicating will entertain as well as inform. More importantly, they will educate, promote democracy, and save lives. And in the process they will also create a lot of new jobs. In fact, they're already doing it.*"[117]

Kedua, orang yang melihat realitas virtual dengan pandangan yang pesimistis, curiga, menolak, *refusal* (**Ian Boal, Gandy, Slouka**). Penolakan terhadap realitas virtual ini terungkap dari apa yang dikemukakan oleh **Slouka** yang melihat abad *cyberspace* sebagai abad yang penuh bahaya, penuh ancaman yang menyuguhkan berbagai kepalsuan, berjuta kesemuan, ketidakpedulian.

---

115 Yasraf Amir Piliang, *op.cit.*, hal. 14-15

116 Howard Rheingold, *op.cit.*

117 Al Gore, *Speech at the Superhighway Summit Royce Hall*, 11 Januari 1993, UCLA Los Angeles, California, versi electronik dapat dijumpai di http://www.eff.org/pub/GII_NII/ Govt_docs/gore_shs.speech. Baca juga artikel Al Gore dengan judul *Bringing Information to The World: The Global Information Infrastructure*, Harvard Journal of Law and Technology, No. 1 Winter 1996.

Realitas virtual oleh **Slouka** juga dicurigai sebagai alat politik oleh kekuatan superpower, proses *Amerikanisasi*, sangat agresif dan destruktif. *Cyberspace* yang menawarkan demokrasi global oleh **Slouka** lebih tepat dikatakan sebagai representasi demokrasi. Meski demikian, Slouka tidak menolak sepenuhnya dunia realitas tersebut. Slouka menolak sikap arogan para pakar dan penganutnya (*net religionist*) yang percaya bahwa segala persoalan manusia dapat dipecahkan oleh teknologi realitas virtual, yang percaya bahwa segala persoalan manusia bahwa setiap dunia fisik dapat di*download* ke dalam komputer dan yang percaya bahwa masa depan manusia bukan di dalam *real life*, melainkan di dalam *virtual reality*.[118]

Ketiga, pandangan yang penuh ketidakpastian, yang mengkritik realitas baru tersebut, tetapi menerimanya sebagai sebuah kenyataan yang tidak dapat ditolak, *fatalistic* (**Baudrillard**). Ketiga pandangan ini didasari oleh sikap yang berbeda dalam melihat realitas virtual dunia *cyberspace* dengan segala perubahan yang radikal di penghujung milenuim kedua.

John Suler dapat dimasukkan dalam kelompok ketiga karena pada satu sisi ia mengungkapkan keoptimisannya seperti yang telah disebutkan di atas, tetapi di sisi lain ia mengungkapkan kekhawatirannya. *Cyberspace* yang dikatakan sebagai *dreamlike world*, yang menempatkan kebutuhan dasar manusia dengan perspektif yang berbeda mengenai pengalaman sendiri dan realitasnya ternyata tidak selamanya ramah.

John Suler mengutarakan kepesimisannya itu dalam ungkapan sebagai berikut:

---

[118] Mark Slouka, *op.cit.*, hal. 47.

> *Cyberspace* is not always benign. It also has the power to inflict frustration, apprehension and stupidity, as revealed in our jokes about computers and the internet. Sometimes, it even fails at its fundamental duty to be interactive, to respond to our needs, resulting in a black hole experience that can draw out the underlying anxieties of those who fall into it.[119]

Pada bagian yang lain ia semakin menegaskan kepesimisannya itu dengan mengatakan

> Computers and the internet are good... or are they? Might people be harmed if they become addicted? Some think that *cyberspace* can damage mental health, and that people with psychological and lifestyle problems tend to use it as an escape or to vent their frustrations on online others. Computer and *cyberspace* addiction is a controversial topic. We can speculate about the features of pathological internet use, but is it a genuine mental disorder?[120]

Terlepas dari kepesimisan mereka, fakta yang terjadi membuktikan bahwa *cyberspace* semakin mantap menampakkan keberadaannya, artinya meskipin kritik tajam datang bertubi-tubi dan menyerangnya dengan berbagai alasan, *cyberspace* sampai sekarang tetap ada dan berkembang melebihi perkembangan yang mungkin oleh para penemunya tidak diperkirakan sebelumnya.

B. DAMPAK PERKEMBANGAN TEKNOLOGI TERHADAP KEHIDUPAN MANUSIA

Kemajuan ilmu pengetahuan dan teknologi selama hampir 60 tahun terakhir ternyata lebih luas dan lebih cepat daripada perkembangan yang dicapai manusia selama 160 tahun sebelumnya. Penemuan senjata nuklir hampir 60 tahun yang lalu di Los Almos, New Mexico, merombak pandangan manusia tentang pemanfaatan teknologi. Teknologi nuklir pada satu sisi membawa

---

119 John Suler, *op.cit.*
120 *Ibid.*

kemajuan yang menjanjikan perbaikan umat manusia (pemanfaatannya sebagai tenaga, energi, pengawetan tanaman dan sebagainya) diimbangi oleh sisi kelamnya yang memungkinkan pemanfaatannya yang dapat memusnahkan peradaban hampir 5 (lima) sampai 6 (enam) kali lipat.

Luas dan kecepatan penemuan di bidang teknologi telah demikian cepatnya sehingga tenggang waktu untuk membahas layak tidaknya suatu temuan baru itu diterapkan pada kehidupan manusia menjadi salah satu persoalan tersendiri. Apa yang layak secara etis dan apa yang tidak layak ditinjau dari segi dampaknya secara kemanusiaan selalu menjadi bahan perbincangan hangat. Bagaimanapun juga kemajuan teknologi cepat atau lambat akan mempengaruhi kaidah-kaidah kebudayaan kita, lembaga-lembaga sosial-budaya kita dan (dari segi sosial politik) pola-pola pengambilan keputusan kebijakan pemerintahan negara kita.[121]

Hampir semua negara meyakini bahwa ilmu pengetahuan dan teknologi adalah salah satu faktor yang penting dalam menopang pertumbuhan dan kemajuan negara.[122] Negara yang tidak memiliki dan menguasai ilmu pengetahuan dan teknologi akan tertinggal dari peradaban. Ilmu pengetahuan dan teknologi sekarang diagung-agungkan dan dijadikan sebagai ideologi. Orang cenderung mendewa-dewakan teknologi seakan-akan teknologi adalah suatu azimat, paspor atau tanda masuk satu-satunya menuju kesejahteraan,

---

[121] Juwono Sudarsono, *Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial-Politik*, Masyarakat: Jurnal Sosialogi, FISIP UI-Gramedia, Jakarta, 1992, hal. 4. Bandingkan dengan Ari Purwadi yang mengatakan Teknologi mewakili suatu sistem nilai tertentu, karena ia merupakan produk sosial budaya dari suatu masyarakat tertentu. Ari Purwadi, *Kebutuhan Akan Perangkat Hukum Perjanjian Di Bidang Alih Teknologi*, Hukum dan Pembangunan, No. 3 Th. XXIII Juni 1993, hal. 234

[122] Dalam konteks pembangungan ekonomi, teknologi dapat berperan sebagai mesin pertumbuhan ekonomi. J. Davidson Frame, *International Business and Global Technology*, DC Heat and Company, Lexington, 1984, hal. 7.

kemakmuran dan keadilan. Tidak hanya itu, teknologi yang dikembangkan ternyata sangat jelas menimbulkan kultus baru dalam teknologi yaitu menimbulkan masyarakat yang konsumtif.[123]

Ada juga mitos yang mengundang banyak simpati terhadap teknologi, yaitu memandang teknologi sebagai alat pembebas, sarana demokrasi dan partisipasi serta dapat mewujudkan otonomi manusia. Anggapan ini masih harus dipertanyakan secara kritis sebab teknologi juga bisa bertindak sebagai belenggu bagi kebebasan manusia. Teknologi dapat menjadi alat pembebas manusia apabila manusia memiliki tradisi praksis yang kritis dan mempraketekkan *practical reason.* Pada saat nilai-nilai kemanusiaan dikorup, dikekang dan dimatikan oleh nilai-nilai yang mementingkan "fungsi" dan "pragmatisme," maka teknologi akan menjadi alat perusak dan penindas yang efektif.[124]

Teknologi canggih dapat memudahkan pertumbuhan kebebasan manusia hanya karena teknologi canggih dapat mengurangi secara radikal ketidaksesuaian dalam hubungan kita dengan lainnya (yang dibatasi oleh dimensi waktu, tempat dan suasana) dan ketegangan yang ditimbulkan oleh ketidaksesuaian ini. Teknologi canggih memudahkan pertumbuhan kebebasan manusia karena teknologi canggih membuat kita tidak perlu lagi dan tidak harus terus bersandar pada saluran-saluran komunikasi dan transportasi yang tidak menentu. Masyarakat atau sekelompok kecil orang dapat berinteraksi secara

---

123 T. Jacob, *Manusia, Ilmu dan Teknologi*, PT. Tiara Wacana, Yogyakarta, 1993, hal. 13

124 Miftah Wirahadikusumah, *Logika dan Gramar Teknologi: Sebuah Tinjauan Psikoanalisis*, Masyarakat: Jurnal Sosiologi, FISIP UI-Gramedia, Jakarta, 1992, hal. 30. Dalam hal teknologi menjadi alat penindas, maka apa yang dilakukan oleh Hitler dan Joseph Stalin yang mengerahkan para saintis dan teknolog dalam upaya membangun negara yang kuat dapat dijadikan contoh. Untuk itu mereka membuat program riset dan pengembangan yang sangat mahal. Hitler mendambakan senjata-senjata super ampuh sementara Stalin memimpikan bom atom. Penggunaan sains untuk keperluan demikian dinamakan sains totaliter.

lebih efektif dan harmonis dalam sistem organisasi yang sangat disederhanakan, tetapi ini hanya mungkin terjadi jika organisasi yang menggunakan teknologi canggih mempunyai semua bahan, teknik dan masukan budaya di tempat itu. Dengan mengurangi perbedaan ruang dan pembagian kerja yang ekstrem, pengawasan hirarki atau birokrasi yang terpusat menjadi tidak berguna.[125]

Di sisi lain terdapat kekhawatiran terhadap perkembangan teknologi seperti ditulis oleh **George Orwell** dalam bukunya *Nineteen Eighty-Four*. Dalam bukunya **George Orwell** mengisahkan betapa kemajuan teknologi telah dipergunakan oleh kekuasaan untuk memasang pengawasan yang amat ketat terhadap semua anggota masyarakat. Semua penghidupan warganegara diatur dari pusat kekuasaan, yang memonopoli segala peralatan teknologi canggih. Tiada lagi warganegara yang berfikir bebas,[126] karena kehidupan menjadi semakin mekanis dengan realita atau fakta yang sudah dapat ditebak sesuai dengan proses mekanistis itu.

Dengan demikian melakukan kegiatan observasi dan penilaian secara kritis atas teknologi sangat diperlukan oleh suatu masyarakat. Hal ini dilakukan melalui peran agen-agen manusia dan aktor sosial. Teknologi yang sebenarnya mengandung arti *automatif* dan alat apabila tidak dipahami secara jelas dan tepat maka manusia menjadi budak dan akan didikte oleh teknologi. Sedangkan pandangan kita tentang teknologi menganggap hanya sebagai alat maka kita akan memperlakukan teknologi tersebut sesuai dengan tuntutan (*demand*) dan kebutuhan (*need*) tertentu demi pencapaian nilai-nilai kemanusaiaan yang tinggi.

---

[125] Eliot D. Chapple, *Mengurangi Pita Merah*, dalam Lewis H. Lapham, *Teknologi Canggih dan Kebebasan Manusia*, Yayasan Obor, Jakarta, 1989, hal. 50

[126] Mochtas Lubis dalam pengantar buku Lewis H. Lapham, *ibid*, hal. x

Pilihan strategis tentang pemilikan dan pengusaaan teknologi yang lebih proporsional dan tepat akan mengarahkan tindakan manusia menuju ke arah yang dicita-citakan itu. Apabila kita memandang teknologi dari aspek *automotif* maka kita akan memperlakukan teknologi sebagai sesuatu hal yang dapat menggantikan berbagai fungsi aktivitas motorik, sensorik dan bahkan mampu mewakili sebagian dari fungsi intelektual.[127]

Sikap pandang yang memperlakukan teknologi sebagai pengganti fungsi-fungsi aktivitas manusia inilah yang telah banyak menimbulkan krisis. Krisis tersebut antara lain adalah krisis rasionalitas yang ditimbulkan oleh kekeliruan proyek besar kemanusiaan di abad *Renaisance* yang terjadi di Eropa Barat dan dimana teknologi itu asalnya diciptakan. Kemudian krisis yang terjadi di Amerika Serikat sebagai tempat di mana teknologi dikembangkan dan berikutnya krisis yang terjadi di Jepang di mana teknologi diproduksi dan dijual di pasar.

Peristiwa yang menghebohkan adalah yang dilakukan oleh **Ned Ludd** di Inggris. Ia dengan keberaniannya yang luar bisa mempengaruhi pekerja lain untuk menghancurkan mesin-mesin penghemat tenaga yang ditakuti akan mengambil alih pekerjaan mereka (yang sekaligus merupakan perlawanan terhadap kekuasaan kapitalis atau pemilik modal di sana). Pada jaman **Luddites** (1812), teknologi baru yang hemat tenaga kerja digunakan dalam industri tekstil di tengah keadaan ekonomi nasional yang secara keseluruhan miskin. Para buruh tekstil yang sudah menghadapi kemungkinan pengangguran besar-besaran, terancam akan kehilangan pekerjaan selamanya mereka dan terancam

---

[127] Miftah Wirahadikusumah, *op.cit*, hal. 29

kehidupan miskin yang hina dina. Dihadapkan dengan pemerintah yang acuh tak acuh serta para pengusaha manufaktur yang buta terhadap keadaan mereka serta kurangnya sarana alternatif untuk merebut kembali pekerjaan mereka atau memperoleh bagian kemakmuran yang dijanjikan oleh produktivitas yang semakin meningkat, para buruh yang dipimpin oleh **Luddite** memberontak dalam keadaan putus asa.[128] **Luddite** kemudian diambil sebagai simbol untuk orang-orang yang menentang teknologi.

Penyebab krisis adalah dominannya *instrumental reason* dengan ciri-ciri *linier, arogance, otoriter, prosedural, sistematik, universal* dan *pragmatik*; dan ditinggalkannya tradisi praksis sebagai kiprah intelektual manusia yang didasari oleh *practical reason* yaitu sikap intelektual dan nilai-nilai manusia secara kritis dan tidak mengenal dikotomi antara teori dan praktek, dikotomi antara ideologi dan teknologi, dikotomi antara *science* dan fiksi dan dikotomi antara rasional dan irasional.[129]

Tidak dapat disangkal oleh siapapun bahwa tingkat perkembangan suatu teknologi memerlukan dukungan pranata nilai budaya dan pranata sosial-ekonomi masyarakat di mana teknologi itu ada dan dikembangkan. Upaya teknologi yaitu upaya untuk menciptakan sistem memerlukan pemahaman akan berbagai sistem kehidupan yang telah ada. Hal ini disebabkan karena sistem ciptaan orang (anggota masyarakat) hanya dapat dibentuk dengan mengubah

---

[128] Berkaitan dengan Luddisme ini, Rosalind Willian menulis dalam *Technology Illustrated* sebagaimana dikutip oleh Jack Golodner, "Karena ancaman kehancuran mesin, para pemilik modal berpikir dua kali sebelum menanamkan modal dalam peralatan baru atau mengurangi upah. Taktik para buruh secara politik tidak sia-sia. Luddisme merupakan suatu faktor penting di balik keputusan Pemerintah Inggris untuk mencabut pemblokiran Eropa Daratan dalam bulan Juni 1812 yang mengakibatkan perbaikan ekonomi secara pesat. Jack Golodner, *Serikat Buruh Amerika Menghadapi Teknologi Canggih*, dalam Lewis H. Lapham, *op.cit*, hal. 75.

[129] Jurgen Habermas, *The Theory of Communicative Action: Reason and the Rationalization of Society*, seperti dikutip oleh Miftah Wirahadikusumah, *op.cit*. hal. 29.

atau mensintesa struktur sistem yang telah ada. Upaya ilmiah menghasilkan pemahaman akan struktur sistem yang ada, oleh karena itu hasil upaya ilmiah menyediakan basis informasi bagi upaya teknologi. Tingkat kemampuan teknologi suatu masyarakat sangat dipengaruhi oleh intensitas upaya ilmiah yang dilakukan oleh masyarakat tersebut yang pada gilirannya sangat dipengaruhi oleh tata nilai budaya yang dianut. Akan tetapi perlu dicatat bahwa suatu masyarakat dengan budaya ilmiah tinggi belum tentu kuat dalam berteknologi.[130]

Pada hakekatnya, teknologi itu mempunyai logika dan *grammar*-nya sendiri yang berhubungan secara erat dan menyatu secara integral dengan kosmologi (sistem nilai kepercayaan) dan *world view* suatu masyarakat yang menemukan (*invent*), memproduksi (*inovative, produce*) dan mengembangkan (*develop*) teknologi tersebut. Kesenjangan, perbedaan, pertentangan atau konflik antara sistem kepercayaan atau kosmologi dan *world view* suatu masyarakat dengan sesuatu bentuk teknologi tertentu yang terdapat di dalam masyarakat tersebut bisa menyebabkan terjadinya berbagai krisis seperti krisis moral dan krisis nilai sosial-budaya.[131]

Untuk menghindari pertentangan atau konflik yang akan berakibat pada krisis moral dan krisis budaya maka perlu dipahami pengertian dan asal-usul sebuah teknologi atau sebuah proses *invention, inovation, development, production* atau *adoption* suatu teknologi. Diperlukan kesadaran intelektual

---

[130] Hal ini dapat terjadi meskipun telah menghargai upaya ilmiah, tata nilai budaya demikian belum tentu mendorong upaya penciptaan sistem-sistem. Sebagai contoh India dan Iran merupakan dua bangsa yang memiliki tradisi ilmiah yang kuat tetapi budaya mereka tidak memicu upaya-upaya teknologi. Hal sebaliknya terjadi di Inggris dan Prancis. Saswinadi Sasmojo dan Sonny Yuliar, *Budaya Sains, Teknologi dan Perubahan Masyarakat*, Seri Penerbitan Sains, Teknologi dan Masyarakat, Edisi I, hal. 35-36

[131] Miftah Wirahadikusumah, *op.cit*, hal. 26-27

yang kritis dan reflektif dari masyarakat yang tidak memisahkan antara sikap nilai ideologi dan teknologi.

Dalam esai *Technology and Science as Ideology* yang dipersembah-kan kepada **H. Marcuse** berkenaan dengan ulang tahunnya yang ke 70, **Habermas** menanggapi jalan buntu yang dialami para pendahulunya. Secara khusus ia menanggapi pendapat **Marcuse** bahwa sains dan teknologi telah menjadi ideologi. Bertolak dari kritik **Marcuse** terhadap rasionalitas **Weber**, **Habermas** menunjukkan bahwa **Marcuse** tetap terbelenggu oleh kerangka pikiran **Marx** yang menjelaskan perkembangan masyarakat melulu dari perkembangan alat-alat produksi. Jalan keluar yang ditawarkan **Marcuse** hanyalah harapan yang mustahil, yakni bahwa sains dan teknologi yang saat ini represif, suatu saat nanti dapat diganti dengan yang tidak represif.[132]

Manusia yang terpikat sains dan teknologi tanpa disadari ditelan kekuasaan sains dan teknologi sebagai sistem total yang menguasai berbagai bidang kehidupan manusia sebagaimana dinyatakan **Marcuse** dalam **A. Widyarsono**:

> Dewasa ini, kekuasaan melestarikan dan memperluas dirinya tidak hanya melalui teknologi melainkan sebagai teknologi, dan teknologi menyediakan legitimasi yang kuat bagi kekuasaan politis yang sedang meluas, yang mengabsorpsi segala bidang kebudayaan.[133]

Marcuse menyimpulkan bahwa rasionalisasi **Weber** tidak hanya merupakan suatu proses jangka panjang perubahan struktur-struktur sosial melainkan juga merupakan rasionalisasi dalam pengertian **Freud**: motif yang

---

[132] A. Widyarsono, *Teknologi dan Sains Sebagai Ideologi (Rasionalisasi Weber menurut Habermas)* dalam Tim Redaksi Driyarkara, *Seri Filsafat Driyarkara: 6 Capita Selecta Diskursus Kemasyarakatan dan Kemanusiaan*, Gramedia, Jakarta, 1993, hal. 90

[133] A. Widyarsono, *Ilmu dan Teknologi Sebagai Ideologi*, LP3ES, Jakarta, 1990, hal. 49

sebenarnya, yakni mempertahankan kekuasaan yang sudah usang, disembunyikan di balik dalih-dalih perintah-perintah rasional bertujuan.[134]

Selanjutnya **Habermas** menjelaskan arti rasionalisasi menurut **Max Weber**. Pertama, perluasan bidang-bidang sosial yang berada di bawah norma-norma pengambilan keputuasan yang rasional. Kedua, indstrialisasi kerja sosial yang mengakibatkan norma-norma tindakan instrumental juga memasuki bidang hidup yang lain. Dari kedua kecenderungan itu terdapat tindakan rasional bertujuan (*Zweckrationales Handeln*) menjadi berlaku umum. Rasionalisasi masyarakat ini berkaitan juga dengan institusionalisasi perkembangan sains dan teknologi yang mengakibatkan legitimasi-legitimasi lama dibongkar.[135]

Untuk merumuskan kembali rasionalisasi **Weber** itu, **Habermas** mengganti pendekatan subjektif yang digunakan **Weber** dan para sosiolog Generasi Pertama Teori Kritis dengan kategori yang lain. Titik tolaknya adalah pembedaan yang mendasar antara kerja dan interaksi sejak jaman primitif. Rekonstruksi ini dilakukan sampai tahap munculnya kesadaran teknokratis yang merupakan hasil rasionalisasi dari atas. Kesadaran teknokratis merupakan ideologi pengganti ideologi borjuis yang mendasarkan diri pada mekanisme pasar bebas dan tenaga-tenaga produktif masyarakat yang dapat berjalan sendiri. Ideologi borjuis tentang kebebasan pasar merupakan pengganti legitimasi-legitimasi mistis, religius dan metafisis dalam masyarakat pra kapitalis. Dalam

---

134 *Ibid*, hal. 93. Pengertian rasionalisasi Weber menunjukkan efek-efek balik kemajuan teknik ilmiah terhadap kerangka kerja institusional masyarakat yang tercakup dalam pengertian modernisasi. Hal ini dilakukan dengan menyusun teori mengenai perubahan institusional yang ditimbulkan oleh perluasan sistem-sistem tindakan rasional-bertujuan, seperti yang dilakukan para sosiolog lain dengan menggunakan istilah-istilah berpasangan, misalnya status dan kontrak, Gemeinschaft dan Gesellschaft, solidaritas yang mekanis dan organis, dan lain-lain.

135 *Ibid*, hal. 91.

arti inilah proses rasionalisasi bersifat *ambigu*. **Adorno** dan **Horkheimer** menganggapnya sebagai dialektika pencerahan, sedangkan **Marcuse** menganggap sebagai ideologisasi sains dan teknologi. Ideologi yang satu menggantikan ideologi yang lain.[136]

Habermas tidak setuju dengan pendapat **Marcuse** bahwa teknologi telah menjadi ideologi. Teknologi sebenarnya merupakan salah satu bentuk rasionalisasi yang dibutuhkan manusia. Proses rasionalisasi dalam masyarakat Barat berjalan timpang karena rasionalisasi dalam bidang kerja yang paling tampak berkembang secara pesat. Sedangkan rasionalisasi dalam bidang interaksi kurang berkembang, bahkan mau digantikan dengan rasionalisasi dalam bidang kerja. Letak watak ideologis "kesadaran teknokratis" ini adalah penghapusan pembedaan antara rasionalisasi dalam bidang interaksi (yang praktis) dengan rasionalisasi dalam bidang kerja (yang teknis dan strategis).[137]

Teknologi dan ilmu pengetahuan mempunyai dua sisi yang berbeda (*ambiguitas*). Pada satu sisi ia telah banyak membantu menyelamatkan, menyehatkan dan memperpanjang usia manusia. Tetapi di sisi lain setiap hari kita mendengar, membaca dan menonton berita mengenai polusi, perusakan lingkungan, pemanasan global, berkurangnya lapisan ozon, hujan asam, penggundulan hutan, perburuan flora dan fauna dan sebagainya. Ilmu pengetahuan dan teknologi yang didewa-dewakan justru membuat manusia makin merasa dirinya dewa sehinggga lupa bahwa salah satu tugas dewa adalah justru melesatrikan kelangsungan hidup.[138]

---

136 *Ibid*, hal 95-107
137 *Ibid*, hal. 111
138 Juwono Sudarsono, *op.cit.*, hal. 6

Teknologi berasal dari bahasa Yunani *technologia* yang artinya pembahasan sistematik tentang seluruh seni dan kerajinan (*systematic treatment of the arts and crafts*). Perkataan tersebut mempunyai akar kata *techne* dan *logos* (perkataan atau pembicaraan). Akar kata *techne* pada jaman Yunani Kuno berarti seni (*art*), kerajinan (*craft*).[139] Dari hal tersebut maka pada jaman Yunani, teknologi diartikan sebagai seni memproduksi alat-alat produksi dan menggunakannya. Kemudian berkembang menjadi penggunaan ilmu pengetahuan sesuai dengan kebutuhan manusia, bahkan ada yang menyebutnya sebagai ketrampilan saja.[140] Teknologi juga dapat diartikan sebagai *the know-how of making things.* Juga dapat diartikan sebagai *the know-how of doing things*, dalam arti kemampuan untuk mengerjakan sesuatu dengan hasil nilai yang tinggi, baik nilai kegunaan maupun nilai jual.[141]

Teknologi diartikan sebagai *the application of scientific knowledge to the production of industrial good and improvement of service.* Dalam arti itulah **B.N. Bhattasali** mengatakan bahwa *the term technology in the English language stands for the application of science to the industrial arts.*[142] Dengan demikian maka teknologi bukanlah ilmu pengetahuan dan juga bukan produk. Teknologi adalah penetapan atau aplikasi ilmu pengetahuan untuk memproduk atau

---

139 Ronny Hanitijo Soemitro, *Hukum dan Perkembangan Ilmu Pengetahuan dan Teknologi di Dalam Masyarakat*, Pidato Pengukuhan pada Upacara Peresmian Penerimaan Jabatan Guru Besar Tetap pada Fakultas Hukum UNDIP, Semarang, 6 Desember 1990, hal. 8

140 H. Daud Silalahi, *Rencana Undang-undang Alih Teknologi: Perbandingan Perspektif*, Prisma, No. 4 Th. XVI, April 1987, hal. 40

141 Marsetio Donoseputro, *Pendidikan, Iptek dan Pembangunan*, Surabaya Post, 3 Agustus 1991, hal. 4

142 Sunaryati Hartono, *Pembahasan Kerta Kerja: Pemindahan Teknologi dan Pengaturannya dalan Peraturan Perundang-undangan*; dalam Seminar Aspek-aspke Hukum Pengalihan Teknologi, dipublikasikan oleh Badan Pembinaan Hukum Nasional, Binacipta, Bandung, 1981, hal. 189

membuat barang dan/atau jasa. Produk tersebut merupakan hasil akhir teknologi, tetapi produk itu sendiri bukanlah teknologi.[143]

Negara-negara yang tergabung dalam Organization on Economic Cooperation and Development (OECD) mengartikan teknologi sebagai berikut *Technology means systematic knowledge for the applications of a process or for the rendering of a service, including any integrally associated managerial and marketing technique*.[144] **Keith Pavitt** mempertegas rumusan teknologi tersebut dengan mengatakan *technological knowledge consist not only access to scientific papers, formulae, blueprints, and hardware. It consist also-and perhaps mainly of what people know and what people can do.*[145]

Pengertian yang lebih luas mengenai teknologi dapat dijumpai dari definisi yang dibuat oleh World Intelectual Property Right (WIPO) yaitu:

> Technology mean systematic knowledge for the manufacture of a product, the application of a process or the rendering a service, whether that knowledge be reflected in an invention, an industrial design, a utility model or a new plat variety, or in technical information or skill, or in the services and the assistance of an industrial plant or the management of an industrial of commercial enterprise or its activities.[146]

Dari beberapat definisi teknologi tersebut di atas, ada beberapa segi atau aspek yang perlu diperhatikan, yaitu:[147]

---

143 Maurice Mountain. *The Continuing Complexities of Technology Transfer*, dalam Gary K. Bertsch dan John R. McIntrye (ed). *National Security and Technology Transfer: The Strategic Dimensious of East-West Trade*, Westview Press Inc, Coloradi, 1983, hal. 8.

144 OECD. *North/South Technology*. Paris. 1981

145 Keith Pavitt, *The Multinational Enterprise and the Transfer of Technology*, dalam Jhon H. Dunning (ed). *The Multinational Enterprise*, George Allen & Unwinn Ltd, London, 1971, hal. 70. Bandingkan dengan James F. Childress yang mendefinisikan teknologi sebgai penerapan sistematis dari pengetahuan ilmiah dan ketrampilan teknis demi pengendalian bahan, energi dan sebagainya untuk tujuan-tujuan praktis. James F. Childress, *Prioritas-prioritas Dalam Etika Biomedis*, Kanisius, Yogyakarta, 1989, hal. 95

146 *WIPO Licencing Guide for Developing Countries*, Geneva, 1977, hal. 28.

147 Ridwan Kairandy, *Francise dan Kaitannya Sebagai Sarana Alih Teknologi: Suatu Tinjauan Hukum*, Jurnal Hukum Ius Quia Iustum FH UII Yogyakarta, No. 7 Vol. 4-1997, hal. 115-116

1. Teknologi terdiri dari informasi yang mampu mengaplikasikan semua tahapan dari perencanaan, organisasi, dan operasi suatu industri atau perusahaan (komersial) dengan segenap aktivitasnya.
2. Teknologi mempunyai kontribusi untuk membuat setiap tahapan yang mencakup perencanaan, organisasi dan operasi kegiatan suatu industri atau perusahaan; maka teknologi tidak hanya terdiri dari scientific knowledge, tetapi juga pengetahuan bisnis atau organisasi
3. Teknologi bisa berupa teknologi yang berwujud (bertubuh) dan tidak berwujud.

Perkembangan teknologi telah mempengaruhi kehidupan manusia bahkan sampai hal-hal yang bersifat pribadi. Dalam hal perkembangan teknologi, **T. Jacob** membagi siklus ilmu pengetahuan dan teknologi menjadi 5 (lima) siklus *kondratieff*, yaitu yang berulang-ulang setiap 50 tahun. Kelima siklus itu adalah:[148]

1. Siklus pertama dimulai dengan revolusi teknologi (1760)
2. Siklus kedua ditandai dengan terbentangnya jaringan kereta api (1848)
3. Siklus ketiga dimulai dengan ban berjalan (1895)
4. Siklus keempat ditandai dengan tenaga atom dan motorisasi masal (1945)
5. Siklus kelima (sekarang) ditandai dengan ciri perkembangan mikroelektronik dan bioteknologi.

Pada tahap awal lembaga teknologi diperlakukan sebagai sesuatu yang statis, tidak berubah oleh keadaan. Pada tahap kedua, lembaga teknologi telah diakui sebagai sesuatu yang berubah atau dinamis, tetapi perubahannya bersifat

---

[148] T. Jacob, *Menuju Teknologi Berperikemanusiaan*, Yayasan Obor Indonesia, Jakarta, 1996, hal. 15.

independent dari perubahan masyarakat, atau dengan istilah lain merupakan suatu variabel *exogenous* dalam model masyarakat. Baru pada tahap ketiga lembaga teknologi diperlakukan sebagai variabel yang *endogenous*. Dengan perkataan lain baru pada tahap ketiga ini diakui bahwa lembaga teknologi berhubungan dengan variabel-variabel sosial-ekonomi lainnya.[149]

Dari uraian di atas dapat dilihat bahwa eksistensi dan fungsi teknologi harus didukung oleh suatu pranata nilai budaya dan pranata sosial ekonomi tertentu di mana teknologi itu diciptakan. Pranata itu juga termasuk tingkat pengetahuan atau tingkat intelek masyarakat yang sesuai. Jadi teknologi itu sifatnya *value ladden*. Ia tidak bebas nilai. Ia berkembang dan didukung oleh kosmologi atau *world view* masyarakat yang menciptakan dan mengasainya.[150]

Setiap teknologi bisa menjadi misteri dan penuh keajaiban jika tidak dilihat secara kritis. Ia akan menjadi monster atau tuyul-tuyul yang magis dan berkuasa. Ia ditakuti sekaligus dikagumi. Lihatlah bangsa Jepang dalam melihat teknologi. Mereka konsisten untuk melakukan *secrutiny* dan *dekonstruksi* terhadap teknologi dalam rangka untuk menguasainya dan memproduksinya, sehingga secara satir ada pameo yang mengatakan bahwa *technology was invented in Europe and developed in USA, but produced as made in Japan.*

---

[149] Ronny Hanitijo Soemitro, *op.cit.*, hal. 23

[150] Banyak orang di Indonesia seperti juga di negara-negara lain berpendapat bahwa teknologi itu netral, akan tetapi banyak teknologi sebenarnya tidak netral, tidak bebas nilai. Teknologi itu sendiri memiliki dampak-dampak yang terbawa sejak lahir dengan pengembangan teknologi itu sendiri. Contoh yang paling menonjol adalah teknologi energi nuklir. Pusat-pusat pembangkit energi listrik adalah sebuah contoh bahwa teknologi itu tidak netral. Pendapat yang berbeda dikemukakan oleh Henry Steele Commager. Ia berpendapat bahwa seperti halnya ilmu pengetahuan, teknologi bersifat netral (bebas nilai). Manusialah yang menerapkannya dan bertanggung jawab atas teknologi. Polio Vitruvius menulis bahwa ciri yang berdaya cipta dan psikis dalam diri manusialah yang melahirkan peradaban, sampai ke Hiroshima, teknologi merupakan sarana utama untuk kemajuan atau bagi kematian. Pernyataan ini memang bertentangan dengan apa yang telah dikemukakan di atas, yaitu teknologi tidak bebas nilai. Lihat lebih lanjut dalam tulisan Henry Steele Commager, *Terkutuklah Segala Yang Mutlak*, dalam Lewis H. Lapham (ed), *op.cit*, hal. 26.

Pertanyaan ini kurang lebih sama bisa juga dilontarkan disini: Bagaimana dengan bangsa Indonesia?[151]

Indonesia sendiri saat ini sedang dan akan terus mengembangkan teknologi untuk berbagai keperluan. Hal ini dilakukan untuk menghadapi tantangan yang semakin menantang di masa mendatang terutama dalam bidang industri dan perdagangan. **Francois Raillon** mengungkapkan dengan baik sekali usaha yang dilakukan Indonesia dalam bidang teknologi ini seperti yang dikatakannya dalam **Nasir Tamara**

> "... bahwa di Indonesia kesadaran akan kebutuhan teknologi bukanlah hal yang baru. Yang baru hanyalah keinginan memacu pemakaiannya sejalan dengan majunya industrialisasi. Pemakaian teknologi dalam setiap produksi menjadi semakin besar; pengusaan atas prosesnya, adanya kemampuan untuk menyesuaikan serta mengembangkan teknologi menjadi kewajiban mendasar."[152]

Dari uraian tersebut sebenarnya ada tiga hal yang ingin dicapai dari pengembangan teknologi itu. *Pertama*, importasi teknologi asing sesuai dengan kebutuhan. *Kedua*, pengembangan teknologi domestik melalui riset dan pengembangan serta menyediakan tenaga ahli (*skill formation*). *Ketiga*, mengubah kesenjangan antara negara maju dengan negara sedang berkembang.[153]

---

151 Miftah Wirahadikusumah, *op.cit.*, hal. 31.

152 Francois Raillon, *Indonesia Tahun 2000 (Tantangan Teknologi dan Industri)*, (terjemahan Nasir Tamara), CV. Haji Masagung, 1990, hal. 54. Pemakaian teknologi ini tidak diikuti dengan kesadaran untuk mengembangkan riset dan pengembangan (research and development) yang menjadi unsur mutlak dalam rencana pengembangan teknologi. Rencana pengembangan teknologi di Indonesia yang diwujudkan dalam kebijakan pemerintah sangat kurang, hal ini dapat terlihat dengan berbagai Ketetapan MPR (seperti TAP MPR No. IV/MPR/1973, TAP MPR No. IV/MPR/1978, TAP MPR No. II/MPR/1983 dan TAP MPR No. II/MPR/1993) yang lebih mengedepankan pemanfaatan teknologi untuk pembangunan dibandingkan dengan riset sains dan teknologi, sehingga tidaklah mengherankan kalau Indonesia tidak mempunyai dasar-dasar pengembangan teknologi seperti yang disinyalir oleh Muhammad Nur.

153 T. Mulya Lubis, *Alih Teknologi: Antara Harapan dan Kenyataan*, Prisma, No. 4 Th. XVI, April 1987, hal. 11.

Upaya mengembangkan teknologi di Indonesia akan berhasil jika tata nilai budaya yang ada di Indonesia mendukung usaha-usaha tersebut. Setidak-tidaknya ada 3 (tiga) ciri penting dari tata nilai budaya yang mendukung kesuburan perkembangan ilmu pengetahuan dan teknologi, yaitu:[154]

1. Menghargai dan menghormati upaya pemahaman akan berbagai fenomena kehidupan.
2. Menghargai upaya pemanfaatan pengetahuan yang dimiliki untuk membentuk sistem-sistem baru
3. Memiliki kriteria untuk memilih upaya-upaya ilmiah dan teknologi yang membawa pada terwujudnya tata kehidupan yang lebih baik
4. Memiliki kriteria yang memungkinkan terwujudnya hubungan sosial yang lebih terbuka, serta terkendalikannya pertumbuhan institusi yang tidak tanggap terhadap permasalahan lingkungannya.

Dengan dilakukan pengembangan teknologi yang terus menerus maka akan timbul penguasaan atas teknologi itu sendiri. Pengusaan teknologi berarti penguasaan atas suatu misteri dan misteri adalah *power*. Arti simbolik dari kekuasaan atau misteri sebagai suatu *power* di jaman dahulu adalah ibarat api. Hal ini dicontohkan dengan **Promotheus** si pembawa api. Ia berdiri tegak di depan manusia-manusia penakluk sesamanya dan penakluk alam.

Pengembangan teknologi di Indonesia betul-betul harus dilakukan dengan memperhatikan berbagai aspek yang dapat ditimbulkan akibat pengembangan itu. Teknologi dan hasil-hasilnya sekarang ini tidak hanya dimanfaatkan untuk kesejahteraan manusia, tetapi sekaligus dapat

---

[154] Saswinadi Sasmojo dan Sonny Yuliar, *op.cit*, hal. 37

menghancurkan kehidupan manusia. Salah satu wujud dari sifat negatif penggunaan teknologi adalah digunakan teknologi dan hasil-hasilnya untuk kejahatan dengan modus operandi yang baru. Kejahatan saiber atau cybercrime, penggunaan kartu kredit secara tidak sah, penggandaan pulsa atau menekan jumlah pulsa telepon dan pencucian uang (*money laundering*) melalui internet merupakan beberapa contoh dari pemanfaatan teknologi untuk kejahatan.

Teknologi itu sendiri sebenarnya tidak jahat, bahkan bisa membantu manusia dalam meningkatkan taraf hidup dan mengubah masyarakat sebagaimana dikatakan oleh **Joseph J. Grau**

> Although technology is changing the social context within which wrongdoing occurs, it does not cause crime; rather, by adding a new dimension to the social situation, it opens new opportunities for expanded freedom and more effective social control. Human beings can use it for good or evil, for legal or illegal purposes.[155]

Sebagai contoh adalah perkembangan teknologi informasi yang telah melipatgandakan kemampuan berkreasi manusia pada batas yang tidak ada toleransinya sama sekali. Percepatan inovasi sekarang dimungkinkan karena terintegrasinya seluruh kemampuan berfikir dan daya imajinasi manusia ke dalam sebuah jaringan internet. Jaringan internet menjadi semacam jembatan penghubung telepatis dari semua manusia ke manusia lain, dengan kecepatan cahaya menembus batas waktu dan batas negara.

Teknologi informasi sama dengan teknologi lain, hanya di sini informasi merupakan komoditas yang diolah dengan teknologi tersebut. Dalam hal ini teknologi mengandung konotasi memiliki nilai ekonomis. Teknologi

---

[155] Joseph J. Grau, *Technology and Criminal Justice*, dalam Roslyn Muraskin & Albert R. Roberts, *Vision For Change - Crime and Justice and in the Twenty-First Century*, Prentice-Hall Inc, A Simon & Schuster Company Upper Saddle River, New Jersey, 1996, hal. 255

pengolah informasi ini memang memiliki nilai jual, seperti teknologi *database* dan *security*, semuanya dapat dijual. Bentuk dari teknologi adalah kumpulan pengetahuan (*knowledge*) yang diimplementasikan dalam tumpukan kertas (*stacked of papers*) atau sekarang dalam bentuk CD-ROM. Tumpukan kertas inilah yang didapatkan jika anda membeli sebuah teknologi dalam bentuk *patent* atau bentuk HaKI (*Intellectual Property Rights*) lainnya.[156]

Indonesia telah mulai memanfaatkan teknologi informasi ini untuk berbagai keperluan, tetapi ada beberapa kendala yang menyebabkan teknologi informasi belum dapat digunakan seoptimal mungkin, yaitu[157]

1. Kurangnya ketersediaan infrastruktur telekomunikasi. Jaringan telepon masih belum tersedia di berbagai tempat di Indonesia. Biaya penggunaan jasa telekomunikasi juga masih mahal. Hal ini dapat diatasi dengan perkembangan telekomunikasi yang semakin canggih dan semakin murah
2. Penetrasi komputer (PC) di Indonesia masih rendah, untuk itu perlu dipikirkan akses ke Internet tanpa melalui komputer pribadi di rumah. Penggunaan *Internet devices* lain seperti *Internet TV* diharapkan dapat menolong, sementara itu akses Internet dapat diperlebar jangakauannya melalui fasilitas di kampus, sekolahan dan bahkan melalui warung Internet.
3. Isi atau *content* yang berbahasa Indonesia masih langka. Hal ini merupakan masalah yang serius sehingga perlu ada upaya atau kegiatan atau inisiatif untuk memperkaya materi yang ditujukan kepada masyarakat Indonesia yang dilakukan secara sadar dan obyektif.

---

[156] Budi Rahardjo, *Implikasi Teknologi dan Internet Terhadap Pendidikan, Bisnis dan Pemerintahan, Siapkah Indonesia?*, Makalah pada seminar di Riau, dapat dijumpai di http://budi.insan.co.id/articles/riau-it.doc.

[157] *Ibid.*

Memang ada kekhawatiran munculnya revolusi teknologi informasi di masa mendatang tidak hanya membawa dampak pada teknologi itu sendiri, tetapi juga akan mempengaruhi aspek kehidupan lain seperti agama, kebudayaan, sosial, politik, kehidupan pribadi dan kehidupan bermasyarakat lainnya. Jaringan informasi global atau internet saat ini menjadi salah satu sarana untuk melakukan kejahatan. Internet menjadi medium bagi pelaku kejahatan untuk melakukan kejahatan dengan sifatnya yang mondial, internasional dan melampaui batas atau kedaulatan suatu negara. *Cross boundaries countries*, menjadi motif yang menarik bagi para penjahat digital.

Kejahatan dan penjahat saat ini menjadi pasangan yang serasi dari kebaikan dan orang baik yang ada dalam masyarakat. Dalam masyarakat modern yang sangat kompleks dan heterogen, perangai anti sosial dan kejahatan itu berkembang dengan cepatnya. Kondisi lingkungan dengan perubahan-perubahan yang cepat, norma-norma dan sanksi sosial yang semakin longgar serta macam-macam subkultur dan kebudayaan asing yang saling berkonflik, semua faktor itu memberikan pengaruh yang mengacau dan memunculkan disorganisasi dalam masyarakatnya. Muncullah banyak kejahatan.[158]

Apa yang berkembang dan dikembangkan oleh teknologi tidak luput dan akan selalu diatur oleh hukum. Perhatian terhadap hukum teknologi itu sendiri saat ini merupakan hal penting sejalan dengan pesatnya perkembangan teknologi yang secara langsung memberi pengaruh terhadap hukum. Pada kenyataannya, piranti hukum yang ada saat ini tidak dapat secara penuh mengimbangi ekses-ekses yang ditimbulkan akibat pemanfaatan teknologi.

---

[158] Kartini Kartono, *Patologi Sosial*, CV. Rajawali, Jakarta, 1983, hal. 167-169

Sebagai contoh perkembangan teknologi informasi akan memberikan pengaruh terhadap bentuk-bentuk perbuatan hukum berdimensi baru.[159]

Sebagian besar teknologi saat ini dikuasai oleh korporasi. Korporasi menggunakan teknologi untuk mencapai tujuan utamanya, yaitu mencari keuntungan sebesar-besarnya. Korporasi dilakukan dengan menggunakan usaha manjerial yang baik, koordinasi produksi yang baik serta pemasaran produk yang terarah pula sehingga dalam sebuah korporasi terdapat sejumlah akumulasi modal yang kuat dan menjadi sumber kekayaan utama dalam pengembangan korporasi. Ia menggunakan teknologi yang ada, pengumpulan modal yang kuat. Mereka membangun jaringan dalam skala yang besar.[160]

Seringkali dalam upayanya untuk memperoleh keuntungan tersebut dilakukan dengan tidak atau kurang memperhatikan dan karenanya merugikan pihak lain seperti lingkungan, konsumen, buruh, masyarakat luas, bahkan negara.[161] Bentuk tindakan itu berupa penggunaan teknologi dan hasil-hasilnya yang dapat merugikan masyarakat luas. Tindakan mereka disebut dengan nama kejahatan korporasi (*corporate crime*).

Dari uraian di atas terlihat bahwa teknologi selain membawa keuntungan berupa meningkatnya taraf kehidupan manusia, juga mempunyai sisi gelap terutama apabila dipakai untuk tujuan kejahatan. Teknologi itu sendiri sebenarnya tidak jahat, yang membuat teknologi itu nampak jahat adalah

---

159 Bentuk-bentuk perbuatan itu antara lain joycomputing, hacking, the trojan horse, data leakage, data diddling, to frustrate data communication, software piracy dan sebagainya. Bentuk kejahatan ini sebelumnya tidak dikenal dalam berbagai sistem hukum sebelum berkembangnya teknologi informasi.

160 Clinard & Yeager, *Corporate Crime*, The Free Press A Division of Mac Millan Publishing Co. Inc, New York, 1980, hal. 1.

161 I.S. Susanto, *Menciptakan Lingkungan Hidup Yang Nyaman*, Pidato Dies Natalis UNDIP ke 40, 15 Oktober 1997, hal. 6

pembuat atau pemakainya yang memang mempunyai tujuan untuk melakukan kejahatan. Jika teknologi informasi memenuhi harapan bisa membawa penggunanya pada kehidupan, kemakmuran dan kesejahteraan yang lebih tinggi maka teknologi informasi itu perlu dikembangkan, tetapi jika perkembangannya akan membawa dampak negatif bagi masyarakat atau penggunanya, maka lupakan saja teknologi informasi, dan kita akan memetik akibatnya berupa ketertinggalan peradaban.

C. MEMAHAMI KEJAHATAN BERDASARKAN PERSPEKTIF KRIMINOLOGI KRITIS

1. Pemahaman Kritis Terhadap Kejahatan

Teknologi selain membawa keuntungan berupa semakin dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahkannya penjahat melakukan kejahatannya. Teknologi juga memberikan pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran dalam kriminologi yang menitikberatkan pada faktor manusia baik secara lahir maupun psikologis.

Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu sendiri telah ada dan muncul sejak permulaan jaman sampai sekarang dan masa yang akan datang. Bentuk-bentuk kejahatan yang adapun semakin hari semakin bervariasi. Suatu hal yang patut untuk diperhatikan adalah bahwa kejahatan sebagai gejala sosial sampai sekarang belum diperhitungkan dan diakui untuk menjadi suatu tradisi atau budaya, padahal jika dibandingkan dengan berbagai budaya yang ada, usia kejahatan tentulah lebih tua.

Kejahatan sebenarnya tumbuh dan berkembang dalam masyarakat, tidak ada kejahatan tanpa masyarakat atau seperti ucapan **Lacassagne** bahwa masyarakat mempunyai penjahat sesuai dengan jasanya.[162] Betapapun kita mengetahui banyak tentang berbagai faktor kejahatan yang ada dalam masyarakat, namun yang pasti adalah bahwa kejahatan merupakan salah satu bentuk perilaku manusia yang terus mengalami perkembangan sejajar dengan perkembangan masyarakat itu sendiri.

Kejahatan telah diterima sebagai suatu fakta, baik pada masyarakat yang paling sederhana (primitif) maupun pada masyarakat yang modern, yang merugikan masyarakat. Kerugian yang ditimbulkan itu dapat berupa kerugian dalam arti materiil maupun moral. Kerugian materiil berupa timbulnya korban kejahatan dan rusak atau musnahnya harta benda serta meningkatnya biaya yang harus dikeluarkan bagi penanggulangannya. Kerugian moral berupa berkurang atau hilangnya kepercayaan masyarakat terhadap pelaksanaan penegakan hukum yang dilakukan oleh aparat penegak hukum.[163]

Sebenarnya banyak faktor yang harus dipertimbangkan dalam membicarakan mengenai kejahatan, sehingga menimbulkan berbagai sudut pandang yang berbeda. Kejahatan tidak bisa dibicarakan hanya dengan memfokuskan pada satu permasalahan saja yang menjadi sebabnya, karena kejahatan merupakan peristiwa yang mempunyai faktor multidimensi yang menjadi penyebabnya dan mempunyai pengertian yang relatif. Menarik sekali apa yang dikemukakan oleh **J.E. Sahetapy** dan **B. Mardjono Reksodiputro**

---

[162] Ucapan Lacasagne sebagaimana dikutip oleh I.S. Susanto, *Kriminologi*, FH UNDIP Semarang, 1995, hal. 32

[163] Romli Atmasasmita, *Capita Selecta Kriminologi*, Armico, Bandung, 1983, hal. 8.

dalam kaitannya dengan kejahatan yang dikaitkan dengan perilaku masyarakat dan ruang serta waktu. Mereka berdua mengatakan

> "berbicara mengenai kejahatan dan penjahat, saya berkesimpulan bahwa kejahatan mengandung konotasi tertentu, merupakan suatu pengertian dan penamaan yang relatif, mengandung variabilitas dan dinamik serta bertalian dengan perbuatan atau tingkah laku (baik aktif maupun pasif), yang dinilai oleh sebagaian mayoritas atau minoritas masyarakat sebagai suatu perbuatan yang anti sosial, suatu perkosaan terhadap skala nilai sosial dan atau perasaan hukum yang hidup dalam masyarakat sesuai dengan ruang dan waktu."[164]

Di lain kesempatan, **J.E. Sahetapy** mengemukakan bahwa persepsi tentang apa itu yang dinamakan kejahatan, tak dapat tiada pasti akan merupakan bahan debat yang kontroversial, seperti apa yang dinamakan cantik atau kecantikan bisa menimbulkan perdebatan atau dikatakan *beauty is in the eye of the beholder*. Jalan yang paling aman untuk mengkaji permasalahan kejahatan dapat ditempuh dengan menghindari diskusi tentang berbagai teori yang masing-masing mempunyai pangkal tolak atau *outlook*-nya serta asumsi yang implikatif sendiri-sendiri.[165]

Senada dengan pendapat **J.E. Sahetay** dan **B. Mardjono Reksodiputro** di atas, **P.J. Fitzgerald** juga mengemukakan bahwa kejahatan itu adalah sesuatu yang relatif, tidak terlepas dari perbedaan waktu dan sudut

---

164 J.E. Sahetapy dan B. Mardjono Reksodiputro, *Paradoks Dalam Kriminologi*, CV. Rajawali, Jakarta, 1983, hal. 167-168

165 J.E. Sahetapy, *Pisau Analisa Kriminologi*, Pidato Pengukuhan Guru Besar di UNAIR Surabaya, 30 Juli 1983, Armico, Bandung, 1984, hal. 9. Tampak di sini bahwa **Sahetapy** bermaksud menghindari keruwetan dalam memahami kejahatan yang terungkap lewat berbagai teori yang dari waktu ke waktu mengalami perubahan. Banyaknya perbedaan persepsi ini disebabkan karena sudut pandang yang digunakan para kriminologist berbeda sebagaimana dikatakan oleh Diane M. DeMelo, " Criminologist have adopted methods of study from varying social and behavioral sciencies. Like other scinetists, criminologists measure and assess crime over time and place. They also measure the characteristics of criminals, crimes, and victim using various methods." Diane M. DeMelo, *Criminology Theory on the Web*, pada bagian pertama yang berjudul *Introduction to Criminological Theory*, dapat dijumpai di http://personal.tmlp.com/ddemelo/crime/intro.html

> capitalist state. To understand crime we have to understand the development of the political economy of capitalist society.[167]

Berbagai faktor yang ada dalam kehidupan di dunia ini dapat atau berpotensi untuk menimbulkan kejahatan, bahkan perbuatan baikpun dapat memicu seseorang untuk melakukan kejahatan. Kejahatan tidak dapat diprediksi kejadiannya, karena ia begitu antik, tidak mempedulikan tempat dan suasana ketika ia hendak muncul dan tidak pula membanding-bandingkan siapa pelaku dan siap korbannya, tidak mengenal kasta atau status sosial pelaku dan korbannya. Ia begitu misterius ketika belum muncul dan ketika muncul ia menjadi bahan yang menarik untuk dibicarakan baik di ruang-ruang seminar, lokakarya, penataran bahkan di warung kopi pinggir jalan.

Pembicaraan mengenai kejahatan pada masa lampau seringkali kehilangan maknanya karena melepaskan diri dari konsepsi masyarakat sebagai suatu totalitas,[168] yaitu lingkungan sosial tempat berlangsungnya kejahatan. Adapun kejahatan sebagai fenomena sosial selalu merupakan kejahatan di dalam

---

[167] Richard Quinney, *Class, State and Crime*, Longman Inc, New York, 1980, hal. 39. Banyaknya faktor-faktor yang menyebabkan timbulnya kejahatan itu menyebabkan upaya untuk memahami, menanggulangi dan memecahkan masalah kejahatan perlu dilakukan dari berbagai segi, oleh karena itulah maka menurut Hoefnagel, kriminologi disebut sebagai ilmu yang bersifat interdisipliner. Ia memanfaatkan dan mengintegrasikan hasil-hasil penemuan dari berbagai disiplin di bidang kemasyarakatan dan perilaku. Mengingat hal tersebut maka kriminologi adalah disiplin yang faktuil dan bukan suatu disiplin yang normatif meskipun mempunyai hubungan istimewa dengan hukum, ialah hukum pidana terutama. Hukum pidana menciptakan kejahatan dengan mengancam suatu perbuatan dengan reaksi berupa pidana, dan rumusan delik dalam hukum pidana inilah yang menjadi ruang pangkal dari kriminologi. G.P. Hoefnagels, sebagaimana dikutip oleh Sudarto. *Hukum dan Hukum Pidana*, pada Bab ke 8 yang berjudul *Sumbangan Kriminologi Untuk Politik Hukum Pidana*, Alumni, Bandung, 1986, hal. 149.

[168] Hal ini tampak nyata jika pembicaraan mengenai kejahatan dilakukan dengan menggunakan paradigma kriminologi klasik dan positif. Kedua paradigma itu lebih menitikberatkan pada faktor-faktor yang bersifat fisik dari si pelaku, baik faktor yang bersifat jasmaniah maupun psikologi. Uraian lebih jelas mengenai kedua pemikiran itu dapat dibaca dalam I.S. Susanto, Kriminologi, FH UNDIP, 1995, Kejahatan Korporasi, BP UNDIP, 1995, Romli Atmasasmita, Teori dan Kapita Selekta Kriminologi dan sebagainya serta lihat juga dalam homepage Dian M. DeMelo, Criminology Theory on the Web, dapat dijumpai di http://personal.tmlp.com/ddemelo/crime/classical.html

pandang masyarakat sebagaimana dikatakan dalam tulisannya *"admitted by different societies at different times take different views about what conduct is right or wrong; and whether a crime is thought wrong in itself or only legally will depend on the moral code current in society".*[166]

Kejahatan merupakan perbuatan anti sosial, tidak hanya terdapat di masyarakat yang sedang berkembang, tetapi ada juga di masyarakat yang sudah maju (dengan peralatan teknologi yang lebih canggih tentunya). Kejahatan tidak hanya ada di dunia nyata (*real*) tetapi ia juga ada di dunia maya (virtual) dengan bentuk yang berbeda dengan wajah kejahatan yang konvensional karena telah diperhalus sedemikian rupa. Keberadaan suatu kejahatan identik dengan keberadaan manusia itu sendiri meskipun ada kemungkinan bentuk atau tipe kejahatan dari tiap-tiap masyarakat berbeda.

Dari uraian di atas maka dapat diketahui bahwa memahami kejahatan dan sebab-sebab terjadinya suatu kejahatan bukanlah suatu persoalan yang sederhana. Kita tidak bisa mengatakan bahwa seseorang melakukan kejahatan karena dendam, lapar atau khilaf saja, tentu ada faktor lain yang ada dibelakang kejadian tersebut. Kompleksnya penyebab terjadinya kejahatan itu karena terkait dengan berbagai faktor sebagaimana **Richard Quinney,**

> The study of crime involves an investigation of such natural product and contradictions of capitalism as alienation, inequality, poverty, unemployment, spiritual malaise, and the economic crisis of the

---

166 P.J. Fitzgerald, *Criminal Law and Punishment*, Clarendon Press, Oxford, 1962, hal. 6. Bandingkan dengan pendapat Leon Radzinowicz yang menyatakan "Crime was a general phenomenon it occurred not merely in all advanced societies whatever type at all stages in their development. There was no sign that it was on the decline. It must therefore be accepted as a social fact a normal part of society, which could not be eradicated at will." Leon Radzinowicz, *Ideology and Crime, A Study of Crime in its Social and Historical Context*, Heinemann Educational Books, London, 1966, hal. 72.

masyarakat sebagai rangkaian dari keseluruhan proses-proses sosial, budaya, politik, ekonomi dan struktur yang ada di dalam masyarakat. Semua itu merupakan hasil sejarah hubungan antar manusia dan untuk selanjutnya ikut mempengaruhi hubungan antar manusia. Dengan demikian untuk memahami masalah kejahatan perlu diperhatikan keseluruhan proses-proses yang terjadi di dalam masyarakat mengingat pengertian kejahatan bersifat relatif dan jauh dari pengertian absolut.[169]

Ketidakberdayaan pemikiran kriminologi klasik dan positive dalam menjelaskan mengenai sebab-sebab kejahatan menyebabkan munculnya aliran pemikiran baru dalam kriminologi yang disebut dengan nama kriminologi kritis Bentuk pemikiran kriminologi kritis terkait dan tidak dapat dipisahkan dari perkembangan struktur masyarakat, artinya kejahatan yang menjadi fokus pembahasan teori kriminologi tidak lagi bersifat bebas nilai (bukan lagi menjadi ilmu murni) karena kejahatan selalu merupakan hasil dari pengaruh dan interaksi berbagai faktor, seperti sosial, budaya, ekonomi dan politik. [170]

Pemikiran kritis dalam sosiologi di Amerika Serikat diilhami oleh hasil karya **C. Wright Mills**, *The Sociological Imagination* (1959) yang menulis mengenai tradisi sosiologi **Marx** dan **Weber** di Eropa, **Veblen** dan **Lynd** di Amerika. Ia juga mengkritik kecenderungan-kecenderungan yang ada

---

[169] I.S. Susanto, *Statistik Kriminal Sebagai Konstruksi Sosial (Penyusunan, Penggunaan dan Penyebarannya, Suatu Studi Kriminologi)*, Ringkasan Disertasi untuk memperoleh Gelar Doktor dalam Ilmu Hukum di UNDIP Semarang, 10 Maret 1990, hal. 1.

[170] Romli Atmasasmita, *op.cit*, hal. 10. Lihat juga I.S. Susanto, *Kriminologi*, *op.cit*, hal. 75. Lahirnya kriminologi kritis ini juga tidak lepas dari peran Stanley Cohen yang menawarkan gagasan tentang pendekatan skeptis dalam studi tentang perilaku menyimpang. Pandangan skeptis melihat sifat politis dari *social control* dalam pengertian betapa undang-undang, peraturan-peraturan, kebiasaan-kebiasaan dan pengendalian serta repressi dapat menciptakan bentuk serta isi dari apa yang dinamakan kriminalitas serta perilaku menyimpang. Sikap skeptis

sebelumnya dalam sosiologi dan menganjurkan studi-studi yang lebih menarik dan imajinatif mengenai masalah-masalah sosial dan politik. Perkembangan pemikiran sosiologi ini juga dibantu dengan bangkitnya kritisisme sosial. Berkembangnya pemikiran baru dalam sosiologi dan bangkitnya kritisisme sosial juga berpengaruh terhadap perkembangan kriminologi.

Sebagaian dari para ahli itu memusatkan perhatian pada pandangan yang bersifat *tripartite* dalam struktur berfikir kriminologis yang berintikan pada *paradigma fungsionalis, symbolic interactionist* dan *paradigma konflik* (**Simecca** dan **Lee**); *personality, cultural* dan *orientasi struktural* (**Wolfgang**); *positivist, reformist* dan *definisi human rights* (**Schwndinger** dan **Schwendinger**); *perspektif value free science, objective law* dan *state morality* (**Grabiner**); *teori positivist, reaksi sosial* dan *teori konflik* (**Taylor**); atau *conservative, liberal clynical* dan *radical criminology* (**Gibbons** dan **Garabedian**). **Richard Quinney** sendiri mengetangahkan analisanya tentang aliran-aliran kriminologis berdasarkan empat klasifikasi yaitu *positivist, interaksionis, fenomenologis* dan *kritis*.[171]

Dari berbagai studi mengenai kriminologi sejak berkembangnya kriminologi kritis ini dapatlah dikatakan bahwa kejahatan adalah hasil dari suatu proses rekayasa manusia baik di bidang sosial, budaya, ekonomi dan politik. Hasil pemikiran tersebut telah mengubah arah dan tujuan kriminologi sehingga kriminologi tidak lagi bersifat *science for science* melainkan *science for the welfare of the society* atau bahkan dikatakan sebagai *science for the interest of*

---

dalam kriminologi berusaha untuk membebaskan diri dari cengkraman asumsi-asumsi biologis dan psikologis seperti yang menjadi fokus studi kriminologi klasik dan positif.

171 Romli Atmasasmita, *Bunga Rampai Kriminologi*, Rajawali Press, Jakarta, 1984, hal. 83-84

the power elite. Dengan semakin berkembangnya kriminologi baru, maka kriminologi baru menurut **Robert F. Meier** mempunyai kewajiban-kewajiban, yaitu:[172]

1. Mengungkapkan tabir hukum pidana, baik sumber-sumber maupun penggunaan-penggunaan, guna menelanjangi kepentingan-kepentingan penguasa
2. Melakukan studi-studi atas alat-alat pengendali sosial, birokrasi dan mass media untuk mengekspose ketersangkutan mereka dalam ideologi elite
3. Mengajukan rumusan-rumusan kejahatan baru, yang dengan mengoreksi ketidakseimbangan hasil pengaruh elite terhadap pembuatan undang-undang juga memasukkan pelanggaran terhadap hak asasi manusi sebagai kejahatan
4. Mempraktekkan teori-teori kriminologi baru (dalam rangka praksis) dengan mencoba mengubah sarana politik dan ekonomi kapitalisme yang ada yang dianggap sebagai biang keladi keadaan sekarang.

Kriminologi kritis lebih mengarahkan untuk mempelajari proses-proses manusia dalam membangun dunianya di mana dia hidup.[173] Aliran pemikiran ini berpendapat bahwa fenomena kejahatan sebagai konstruksi sosial, artinya

---

[172] Soerjono Soekanto. dkk. *op.cit*, hal. 64-65. Bandingkan dengan I.S. Susanto yang mengatakan bahwa tugas kriminologi kritis adalah menganalisis proses-proses bagaimana cap jahat tersebut diterapkan terhadap tindakan dan orang-orang tertentu. Bandingkan pula dengan pendapat Romli Atmasasmita (didasarkan pada pendapat Marc Ancel mengena la defense sociale) yang mengatakan bahwa kriminologi harus merupakan suatu kontrol sosial terhadap kebijakan dalam pelaksanaan hukum pidana, dengan kata lain kriminologi harus memiliki peran yang antisipatif terhadap semua kebijakan di lapangan hukum pidana sehingga dengan demikian dapat dicegah kemungkinan timbulnya akibat-akibat yang merugikan baik bagi pelaku, korban kejahatan maupun masyarakat pada umumnya. Romli Atmasasmita, *op.cit*, hal, 10-11.

[173] Kriminologi kritis ini mempelajari proses-proses di mana kumpulan tertentu dari orang-orang dan tindakan-tindakan ditunjuk sebagai kriminal pada waktu dan tempat tertentu. Kriminologi kritis bukan sekedar mempelajari perilaku dari orang-orang yang didefinisikan sebagai kejahatan, tetapi juga perilaku dari agen-agen kontrol sosial (aparat penegak hukum), di samping mempertanyakan dijadikannya tindakan-tindakan tertentu sebagai kejahatan. Tingkat kejahatan dan ciri-ciri pelaku menurut kriminologi kritis terutama ditentukan oleh bagaimana undang-undang disusun dan dijalankan. I.S. Susanto, *Kejahatan Korporasi, op.cit*, hal. 8

manakala masyarakat mendefinisikan tindakan tertentu sebagai kejahatan maka orang-orang tertentu memenuhi batasan sebagai kejahatan. Kejahatan dan penjahat bukanlah fenomena yang berdiri sendiri sebab ia ada hanya karena hal itu dinyatakan sebagai demikian oleh masyarakat.[174]

Kriminologi kritis atau kriminologi baru ini memperlihatkan permasalahan-permasalahan pokok untuk dianalisa sebagai berikut:[175]

1. Tekanan perhatian lebih pada akibat-akibat serta reaksi-reaksi sosial penyimpangan
2. Ukuran menyimpang atau tidaknya suatu perbuatan ditentukan bukan oleh nilai-nilai dan norma-norma yang dianggap sah oleh mereka yang duduk pada posisi-posisi kekuasaan atau kewibawaan, melainkan oleh besar kecilnya kerugian atau keparahan sosial (*social injures*) yang ditimbulkan oleh perbuatan tersebut dan dikaji dalam konteks ketidakmerataan kekuasaan dan kemakmuran dalam masyarakat.
3. Perilaku menyimpang sebagai proses sosial dianggap terjadi sebagai reaksi terhadap kehidupan kelas seseorang
4. Usaha pengendalian sosial ditempatkan dalam kerangka mengurangi ketidakadilan struktural.

Dalam kriminologi kritis, nilai-nilai, norma-norma dan adat istiadat yang ada di masyarakat baik yang melembaga atau yang tidak melembaga dipertanyakan, sedangkan keadilan dan hak asasi manusia (sebagai nilai-nilai yang universal) dipandang sebagai nilai-nilai utama dan dijadikan acuan dalam

---

[174] *Ibid.* Bandingkan dengan pendapat David M. Gordon yang menyatakan bahwa kejahatan adalah respon-respon rasional terhadap bekerjanya sistem ekonomi dominan yang ditandai oleh persaingan serta berbagai bentuk ketidakmerataan. Pelaku kejahatan adalah orang-orang yang bertindak secara rasional untuk bereaksi terhadap kondisi-kondisi kehidupan golongan sosialnya di masyarakat. David M. Gordon dalam Mulyana W. Kusumah, *op.cit*, hal. 37

[175] Soerjono Soekanto et.al, *op.cit*, hal. 56-57

menentukan batasan kejahatan. Penganut aliran ini menyerang rumusan kejahatan yang bersifat legalistik dengan mengajukan rumusan kejahatan yang lebih humanis.[176] Kejahatan dirumuskan kembali sebagai setiap tindakan, pranata sosial atau sistem sosial yang melanggar hak asasi manusia, di mana hak itu meliputi hak atas persamaan ekonomi, ras, seks dan berpolitik atau berdemokrasi.

Permasalahan pokok kriminologi kritis yang ketiga dan keempat menyebabkan kriminologi kritis ini disamakan dan disebut dengan istilah kriminologi Marxis atau sosialis.[177] Meskipun ada persamaan dengan pemikiran **Marx** mengenai perjuangan kelas, tetapi tidaklah dapat dipersamakan begitu saja tanpa melihat akar permasalahan yang secara mendasar sangat berbeda jauh titik tolaknya.[178]

---

176 Rumusan kejahatan yang legalistik ini terutama diserang oleh Jock Young dalam karyanya The Working Class Criminology. Young menegaskan bahwa strategi radikal kriminologis bukanlah mendukung legalitas atau rule of law, melainkan membuka kedok hukum dalam warna yang sebenarnya, sebagai alat kelas yang berkuasa dan secara taktis menunjukkan bahwa negara akan melanggar undang-undangnya sendiri, bahwa lgitimasi adalah sebuah dalih belaka, serta pembuat aturan-aturan seringkali adalah pelanggar hukum yang utama. Radikalisme ini terlihat dan ditemukan dalam perjuangan-perjuangan politik berupa gerakan hak-hak sipil, gerakan mahasiswa dan sebagainya yang akhirnya adalah menegaskan bahwa negara menjadi sasaran tujuan dari penelitian kriminologi sebagai pranata kriminogenik karena ketersangkutan dalam korupsi, penipuan, crime of genocide dan mengungkapkan ketidakadilan dalam sistem peradilan pidana.

177 Pemahaman inilah yang menyebabkan **J.E. Sahetapy** tidak setuju dengan apa yang dinamakan kriminologi kritis, meskipun ia mengaku pemikiran ini ada manfaatnya. Bukan hanya karena kriminologi kritis ini bernafaskan Marxisme (sehingga sering dikatakan kriminologi kritis sebagai kriminologi marxis meskipun sebenarnya tidak sama pengertiannya di antara keduanya) atau karena pendirian kriminologi radikal tetapi sedikit banyak bertentangan dengan Pancasila, melainkan juga karena adanya larangan menyebarkan faham Marxisme. Penolakan ini dipertegas dengan mengutip tulisan **Clark B. Klockars** (*We are believe, in the late phase of Marxist criminology, a pont at which its capacity for contribution is exhausted, and where it must confront the reality of its own theoritical and empirical poverty or wither and die*) dan **Jackson Toby** (*the New Criminology is not new* dalam *The New Criminology is the Old Baloney*). J.E. Sahetapy, *op.cit*, hal. 47

178 Pandangan yang keliru itu menyebabkan penilaian terhadap kriminologi kritis juga tidak tepat. Dikatakannya kriminologi kritis saat ini sedang mengalami krisis dan amburadul sejak adanya *perestroijka* dan *glasnost* serta tumbangnya rezim-rezim komunis di Eropa Timur, padahal dalam kenyataannya pada masa reformasi ini di Indonesia, kriminologi kritis dengan pemikiran kritisnya semakin berkembang. Jadi kriminologi kritis bukanlah *The New Criminology is the Old Baloney* (suatu omong kosong belaka), tetapi memang betul-betul ungkapan, ucapan atau tindakan yang betul-betul bermakna.

Apa yang dipermasalahkan mengenai penyamaan makna kriminologi Marxis dan kriminologi kritis (terutama oleh **Sahetapy**) sebenarnya adalah mengenai teori konflik. Dalam perspektif pendekatan kritis, secara relatif dapat dibedakan antara pendekatan konflik dan interaksionis. Pendekatan yang dipakai dalam teori konflik lebih memfokuskan studinya dengan mempertanyakan kekuasaan dalam mendefiniskan kejahatan. Orang berbeda karena memiliki peberdaan kekuasaan dalam mempengaruhi perbuatan dan bekerjanya hukum. Mereka yang mempunyai kedudukan atau kekuasaan yang lebih tinggi akan mempunyai keuntungan dalam mendefinisikan perbuatan yang bertentangan dengan nilai dan kepentingannya sebagai kejahatan dan dapat mencegah tindakan-tindakannya (yang merugikan kelas atau golongan lain terutama golongan masyarakat yang tidak memiliki atau kecil kekuasaannya) menjadi kejahatan.[179]

Dalam pendefinisian suatu perbuatan sebagai kejahatan berarti ada pertentangan konflik antar kelompok. Masing-masing kelompok ingin mempertahankan eksistensinya sehingga berusaha agar tindakannya dalam menjaga eksistensinya itu tetap dapat dilindungi oleh hukum. Meskipun teori ini berpandangan bahwa masyarakat adalah kumpulan kelompok-kelompok yang secara bersama-sama memikul perubahan, namun setiap kelompok dalam masyarakat akan selalu menjaga keseimbangan dalam proses perubahan itu

---

[179] I.S. Susanto, *Kejahatan Korporasi*, *op.cit*, hal. 10. Bandingkan dengan pendapat **William J. Chamblis** yang secara khusus membahas mengenai isi dan bekerjanya hukum pidana, konsekuensi kejahatan bagi masyarakat dan sebab musabab kejahatan. Mengenai sebab musabab kejahatan ia mengemukakan bahwa kejahatan atau bukan kejahatan berasal dari orang-orang yang bertindak secara rasional sesuai dengan posisi kelasnya. Kejahatan adalah suatu reaksi atas kondisi kehidupan kelas seseorang dan senantiasa berbeda-beda tergantung pada struktur-struktur politik dan ekonomi masyarakat. Mulyana W. Kusumah, *Kriminologi dan Masalah Kejahatan (Suatu Pengantar Ringkas)*, Armico, Bandung, 1984, hal. 34.

terutama dalam menghadapi goncangan atau usaha-usaha dari kelompok lain yang berusaha menggesernya.

Pada tahun 1970-an muncul kriminologi Marxis. Meskipun banyak yang menentangnya tetapi para penganutnya mulai mengembangkan ajaran-ajaran Marx mengenai perjuangan kelas. Salah satu penentangnya dalah **Paul Q. Hirst** yang mengatakan bahwa tidak ada teori Marxis tentang kejahatan baik dalam eksistensinya maupun yang dapat dikembangkan dari Marxisme yang ortodoks.[180]

Asumsi-asumsi yang dikembangkan oleh teori konflik adalah sebagai berikut:

1. Segala sesuatu di dalam masyarakat dapat berubah
2. Dalam segala hal, masyarakat menunjukkan adanya dissensus dan konflik
3. Setiap anasir di dalam masyarakat dapat membantu ke arah perubahan
4. Masyarakat didasarkan pada paksaan oleh sejumlah warganegara atas warganegara yang lain.

Perspektif konflik dalam kaitannya dengan hukum dan masyarakat menekankan pada sifat memaksa dan represif dari sistem hukum. Sistem hukum tidak dipandang sebagai alat yang tidak berpihak bagi penyelesaian sengketa, malainkan suatu mekanisme bagi mereka yang mempunyai jumlah kekuasaan paling besar untuk memajukan kepentingan-kepentingannya.[181]

Kriminologi Marxis merupakan salah satu usaha mengembangkan teori konflik, artinya akar dari teori Marxis tentang kejahatan adalah teori konflik. Pengembangan teori konflik yang non Marxis juga ada dan sangat berbeda

---

180 *Ibid*, hal. 11
181 Mulyana W. Kusumah, *op.cit*, hal. 13.

dengan teori konflik yang Marxis meskipun ada ahli yang mencampuradukkan keduanya seperti yang dilakukan oleh **Reid** dan **Allen.** **Reid** mendasarkan teori konflik berdasarkan pada tiga hal, pertama perbedaan bekerjanya hukum mencerminkan kepentingan dari *rulling class*, kedua kejahatan merupakan akibat dari cara produksi dalam masyarakat dan ketiga hukum pidana dibuat untuk mencapai kepentingan ekonomi dari rulling class. Konsep *rulling class* tidak digunakan oleh pendukung teori konflik yang non Marxis seperti **Sellin, Vold** dan **Turk.**[182]

Menurut kriminologi Marxis, kejahatan bersifat patologis. Perilaku yang patologis tersebut berupa batasan alamiah sebagai perbuatan yang merugikan masyarakat atau tindakan yang memperkosa hak-hak asasi manusia dan dapat meliputi kejahatan-kejahatan lapis bawah, di mana orang-orang miskin merupakan sasaran di antara mereka sendiri dan juga lainya maupun kejahatan-kejahatan lapis atas seperti pencemaran, perang daneksploitasi terhadap kelas pekerja. Bagi kriminologi Marxis tindakan yang merugikan masyarakat, yang memperkosa hak-hak asasi manusia tidak dilihat sebagai normal akan tetapi merupakan produk yang bersifat patologis dari sistem ekonomi yang patologis.[183]

Teori konflik yang non Marxis menunjukkan bahwa hubungan kekuasaan yang tidak seimbang mendasari terjadinya kriminalisasi atas perilaku tertentu dibandingkan dengan yang lainnya dan tentu saja dapat mengarah pada keinginan untuk mengubah hubungan tersebut. Hal ini dapat membawa analisis yang obyektif proses kriminalisasi ke arah usaha yang bersifat politis dalam

---

182 I.S. Susanto, *op.cit.* hal.11
183 *Ibid.* hal 12

membantu kelompok yang lemah dalam perjuangannya menghadapi kelompok yang sangat kuar. Kejahatan dipandang sebagai tindakan normal dari orang-orang yang normal yang tidak memiliki kekuasaan yang cukup untuk mengontrol proses kriminalisasi dan dalam perspektif perilaku menyimpang, kejahatan dipandang sebagai perwujudan kebutuhan masyarakat untuk mengkriminalisasikan perbedaan. Nilai dari teori konflik ini adalah pandangannya bahwa di dalam setiap masyarakat selalu terdapat konflik nilai-nilai dan kepentingan-kepentingan di antara bagian-bagian di dalam masyarakat dan penyelesaian dari pertentangan atau konflik tersebut akan dipengaruhi oleh kekuasaan (*power*) dari kelompok-kelompok yang bertentangan. Penyelesaian konflik sesuai dengan tuntutan masyarakat modern dilakukan melalui hukum, baik melalui pembuatan perundang-undangan maupun melalui bekerjanya hukum.[184]

Secara lebih umum, **Ian Taylor, Paul Walton** dan **Jock Young** mengemukakan bahwa kejahatan harus dikaji dengan melihat aspek-aspek yang lebih luas, seperti:[185]

1. *The wider origins of the deviant act.*

   Aspek pertama dalam mengkaji kejahatan yang harus diperhatikan adalah hubungan antara kejahatan dengan sumber-sumber struktural yang lebih mendasar, seperti ketidakmerataan pemilikan sumberdaya-sumberdaya pokok. Konflik-konflik struktural yang ada dalam masyarakat menemptkan perilaku menyimpang dalam konteks ketidakmerataan kekuasaan,

---

[184] *Ibid*, hal. 11-12

[185] Uraian lebih lengkap dan jelas dapat dilihat pada Ian Taylor, Paul Walton dan Jock Young, *loc.cit*, hal. 270-278. Lihat juga Mulyana W. Kusumah, *op.cit*, hal. 38-39

kemakmuran dan otoritas serta menghubungkannya dengan perubahan-perubahan ekonomi dan politik dalam masyarakat atau dalam istilah mereka pengungkapan *a political economy of crime.*

2. *Immediate origins of the deviant act*

Pengkajian masalah kejahatan akan lebih jelas, lengkap dan menyeluruh apabila pengkajian itu meliputi sumber-sumber langsung dari kejahatan. Masalah umum berkaitan dengan tipe penyimpangan tertentu dengan melihat dan menjelaskan faktor-faktor pencetus yang langsung dalam perilaku menyimpang, sebagai akibat tanggapan, reaksi dan pemanfaatan tuntutan-tuntutan strukturil dalam pengertian bahwa manusia memang secara sadar memilih jalan menyimpang sebagai cara pemecahan masalah-masalah eksistensinya dalam suatu masyarakat yang kontradiktif. Hal ini menurut mereka memerlukan *a social psychology of crime.*

3. *The actual act*

Kejahatan tidak dapat terjadi dan dijelaskan begitu saja, karena hubungan antara kejahatan dengan berbagai faktor yang ada dalam masyarakat, hubungan antara keyakinan dengan tindakan antara rasionalitas optimum yang dipilih manusia dengan perilaku yang sesungguhnya dilakukan sangat kompleks. Penjelasan atau pemahaman mengenai kejahatan dalam hal ini dilakukan dengan melihat dinamika sosial atau tindakan nyata yang melatarbelakangi terjadinya kejahatan

4. *Immediate origins of social reaction*

Penjelasan mengenai kejahatan yang terjadi dalam hubungannya dengan sikap masyarakat dalam hal ini perlu dijelaskan. Reaksi sosial yang

dilakukan oleh orang-orang lain, kelompok-kelompok atau alat-alat social control terhadap pelaku penyimpangan dengan melihat bentuk, sifat dan luasnya reaksi sosial. Penjelasan ini dapat diperoleh dengan melihat dan mengkaji serta menganalisa reaksi-reaksi masyarakat yang langsung dialami oleh pelaku kejahatan. Bagaimana reaksi masyarakat terhadap penjahat dan kejahatannya merupakan hal yang penting dalam pembahasan kriminologi kritis dan yang diperlukan di sini adalah *a social psychology of social reaction.*

5. *Wider origins of deviant action*

Reaksi sosial masyarakat seperti disebutkan di atas tidak datang begitu saja, tidak datang dari langit (*taken for granted*). Reaksi sosial yang diberikan masyarakat pada penjahat dan kejahatannya berkaitan dengan latar belakang ekonomi, sosial dan politik yang melandasi bekerjanya reaksi sosial resmi (bekerjanya kekuatan-kekeuatan ekonomi, sosial dan politik yang mempengaruhi keputusan atau kebijakan lembaga-lembaga resmi yang berkaitan dengan penanganan kejahatan) maupun dari masyarakat untuk mengendalikan tingkat kejahatan di lingkungannya.

6. *The outcome of the social reaction on deviant's further action*

Akibat dari reaksi sosial yang datang dari masyarakat terhadap penjahat dan kejahatannya perlu dikaji lebih lanjut, artinya apakah reaksi yang ditimbulkan itu menimbulkan pengaruh bagi penjahatnya itu dan anggota masyarakat yang lain atau tidak. Perlu dilihat sejauh mana pelaku kejahatan secara sadar memberikan reaksi balik atau reaksi masyarakat itu, artinya

apakah si penjahat itu menjadi sadar atas perilaku negatifnya itu atau reaksi masyarakat itu justru membuatnya semakin jahat.

7. *The nature of the deviant process as a whole.*

Kejahatan yang terjadi mempunyai akar permasalahan yang kompleks. Pengkajian terhadap sifat dari proses kejahatan sebagai keseluruhan harus dilakukan dalam suatu hubungan dialektis satu sama lain dari berbagai faktor tersebut di atas. Pembahasan dengan menggunakan hubungan dialektis ini sesuai dengan anjuran dari **William C. Chambliss** yang menyarankan menggunakan metode dialektik dan teori tentang kontradiksi-kontradiksi struktur sebagai titik tolak kriminologi yang terpadu. Dengan menggunakan metode ini ditegaskan bahwa di dalam setiap sistem ekonomi, sosial dan politik terdapat kontradiksi-kontradiksi mendasar dan orang bertindak secara sadar walaupun dihambat oleh warisan tradisi, kepercayaan, pranata-pranata yang ada untuk mengatasi krontradiksi-kontradiksi ini. Dikatakan oleh **Chambliss** "*We must understand the political, economic and social forces leading to differences in crime rates in different historical periods as well as differences between countries in the same period*".[186]

Richard Quinney menyatakan bahwa bentuk pikiran dialektis ini memungkinkan kita untuk mempertanyakan pengalaman masa kini. Bila kita mampu memikirkan alternatif, kita bisa memahami keberadaan masa sekarang dengan lebih baik. Kita tidak tertarik untuk mencari realitas obyektif, kita lebih tertarik untuk menolak tatanan yang sudah mapan, yang akan membuat kita mampu memahami apa yang kita alami dengan lebih

---

[186] Chambliss dalam Mulyana W. Kusumah, *op.cit*, hal. 36

baik. Dengan menerapkan dialektika ini dalam pikiran kita, kita dapat memahami dan melampaui masa kini.[187]

Apa yang diungkapkan oleh **Ian Taylor, Paul Walton** dan **Jock Young** dalam dua karya mereka, yaitu *The New Criminology: for a Social Theory of Deviance* dan *Critical Criminology*, mendapat kritik dari **Paul Moedikdo** terutama ditujukan kepada apa yang telah yang berkaitan dengan pernyataan bahwa kejahatan atau penyimpangan itu adalah normal dalam suatu masyarakat dan tak perlu dikriminalisasi. Dikatakan oleh **Paul Moedikdo** bahwa perumusan itu tidak dapat dipertanggungjawabkan. Hal ini diajukan oleh para teoritisi asal *middle class* karena rasa ketidakberdayaan mereka untuk mempengaruhi negara, budaya dan politik sehingga mereka sampai pada suatu penyanjungan dalam analisa mereka mengenai perilaku menyimpang dan membuat suatu gambaran yang diromantisir mengenai kejahatan, padahal tak ada suatu masyarakatpun yang mentolerir kejahatan kecuali mungkin dalam masyarakat yang membenarkan hukum dari yang paling kuat.[188]

Hal ini tidak mengurangi fakta bahwa ada sejumlah pelanggaran hukum yang dapat dipandang sebagai pernyataan kelangkaan dan kebutuhan yang ditimbulkan oleh struktur masyarakat. Kejahatan atas harta benda dapat didorong oleh nafsu ingin memiliki yang diakibatkan oleh saran produksi dan reklame kapitalis. Kejahatan dengan kekerasan dapat merupakan *way out* rasa harga diri yang frustrasi dalam masyarakat yang mempertahankan

---

187 Richard Quinney, *op.cit*, hal. 13

188 Percakapan Paul Moedikdo dengan Mulyana W. Kusumah, 22 Agustus 1978 yang menunjuk kritiknya yang ditulis dalam Kelk, Constantjin, ed., *Recht, Macht en Manipulatie* (Utrecht/Antwerpen: Het Spectrum, 1976), hal. 1140-141, dapat juga dilihat dalam Mulyana W. Kusumah, *Aneka Permasalahan Dalam Ruang Lingkup Kriminologi*, Alumni, Bandung, 1981, hal. 36-37

penterbelakangan sosial yang tidak teratasi, akan tetapi mempropagandakan harkat yang sama dari manusia.[189]

Paul Moedikdo juga melontarkan kritik terhadap pernyataan **Ian Taylor** dan kawan-kawan mengenai rumusan kewajiban ahli kriminologi untuk berusaha menciptakan suatu masyarakat di mana kenyataan-kenyataan kebhinekaan manusia tidak menjadi korban kriminalisasi penguasa yang dinilainya merupakan rumusan yang berlebihan dan tidak tepat. Bukan kekuasaan untuk mengkriminalisasi kejahatan yang harus dihilangkan, melainkan karakter kelas dari perumusan kejahatan. Kejahatan harus dirumuskan dan diperlakukan atas dasar prinsip-prinsip egalitarian dan koperatif bukan berdasarkan prinsip-prinsip hierarchical dan eksploitatif.[190]

Kritikan **Paul Moedikdo** itu mendapat tanggapan dari **W.H. Nagel**. Ia tidak begitu menaruh perhatian untuk mengurus bagaimana seharusnya para pemegang kekuasaan bertindak, ia lebih menekankan suatu *independent struggle for emancipation*, karena baginya orientasi studi kriminologi adalah ke arah pembebasan rakyat tertindak dan pembebasan dari kekuasaan superior individu serta negara. Simpatinya pada perjuangan pembebasan ini nampak jelas sekali terlihat dalam sikapnya terhadap terorisme oleh individu-individu sebagai reaksi yang dapat dipahami terhadap terorisme yang dilakukan oleh negara. Sikap ini menggejala di Jerman seperti yang terdapat dalam tulisan **Henrich Boel** dan **Guenther Grass** yang mengatakan bahwa kekerasan (kaum terror) hanya gejala

---

[189] *Ibid*

[190] Kritik ini terdapat dalam Paul Moedikdo, *Criminology and Politicization*, dalam C.W.C. Jasperce, et.al, *Criminology: Between the Rule of Law and The Out-laws*, Volume in Honour of Willem H. Nagel, Deventer: Kluwer, 1976, hal. 117, sebagaimana dikutip oleh Mulyana W. Kusumah, *op.cit*. hal. 37-38

belaka, bahwa motivasi terdalam para teror itu harus dicari dari sakitnya masyarakat itu sendiri dan inilah justru menjadi tugas dan kewajiban para penulis dan pemikir untuk kritis terhadap setiap masyarakat dan memperlihatkan penyakitnya.[191] Hal ini seperti inilah yang sebenarnya menjadi perhatian dari **Taylor, Walton** dan **Jock** dalam ungkapannya mengenai *the wider origins of the deviant act, immediate origins of social reaction* dan *wider origins of deviant action* seperti telah diterangkan di muka.

Kriminologi kritis meminjam dari falsafah fenomenologi asmumsi yang rasional bahwa seseorang yang berpokir selalu dalam konteks tempat dan waktu. Pemikiran fenomenologis menurut **Richard Quinney** diawali dengan melihat bagaimana kita memahami dunia. Penjelasan sebagai suatu bentuk pemikiran itu sendiri harus diuji. Para ahli fenomenologis mencurahkan perhatiannya pada masalah filosofis epistemologi dan ontologi. Mereka sepakat bahwa pengetahuan tentang dunia fisik berasal dari pengalaman, tetapi ketika berbicara dunia fisik, seorang fenomenologist tidak dibatasi oleh pengalaman yang benar-benar dialami dan mereka bisa saja berbicara tentang pengalaman yang mungkin dialami sehingga mereka bisa mengubah persepsi tentang berbagai hal dalam dunia.

Para fenomenologis bisa juga bergerak dengan mengisolasi masalah realitas yang obyektif agar dapat mengarahkan perhatian pada realitas yang mewujudkan dirinya langsung dalam kesaradan. Kesadaran itu sendiri diperoleh melalui pemahaman tentang dunia. Pengetahuan tentang dunia tidak dapat terpisah dari pengertian tentang hal-hal yang ada. Setiap pemahaman benda

---

[191] *Ibid*, hal. 38

obyektif yang muncul hanya melalui kesadaran tentang hal tersebut. Realitas harus ditemukan dalam kesadaran kita tentang realitas tersebut. Esensi atau hal yang inti dengan demikian adalah apa yang kita pahami melalui kesadaran dalam pengalamannya di dunia. Setiap obyektivitas harus dicapai melalui subyektivitas kita yaitu melalui kesadaran kita.

Menurut kriminologi kritis, kita tidak perlu selalu berfikir secara kausal meskipun ada berbagai gaya berfikir kausa. Jika kita berfikir secara kausal maka hal itu didasarkan pada apa yang dinamakan oleh **Quinney** sebagai *the social reality by man*. Realitas sosial adalah sesuatu yang bermakna dan bertalian dengan interpretasi tentang situasi. Dalam kaitannya dengan kejahatan, **Quinney** menyatakan bahwa kejahatan adalah suatu rumusan tentang perilaku manusia yang diciptakan alat-alat berwenang dalam suatu masyarakat yang secara politis terorganisasi dan kejahatan adalah suatu rumusan perilaku yang diberikan terhadap sejumlah orang oleh orang-orang lain dengan begitu kejahatan adalah suatu yang diciptakan.

Dalam bukunya *Criminology: Analysis and Critique of Crime in the United States*, **Richard Quinney** mengajukan teori mengenai realitas sosial kejahatan yang bermaksud untuk mengintegrasikan kebhinekaan kriminologi teoritis ke dalam suatu teori kejahatan. Proposisi-proposisi yang merupakan dasar teori ini adalah sebagai berikut:

1. Kejahatan adalah suatu definisi hukum yang diciptakan oleh alat-alat kelas dominan di dalam masyarakat yang secara politis terorganisasi

   Kejahatan adalah suatu rumusan hukum mengenai kelakuan manusia oleh alat-alat kelas dominan dalam masyarakat (anggota-anggota badan legislatif,

polisi, jaksa dan hakim) sebagai wakil-wakil dari kelas penguasa dalam masyarakat, bertanggungjawab atas perumusan dan pelaksanaan hukum pidana. Dengan demikian realitas sosial kejahatan bukanlah sesuatu yang melekat (*inherent*) dalam perilaku melainkan lebih merupakan suatu penilaian yang dibuat oleh suatu pihak terhadap tindakan-tindakan dan ciri-ciri pihak lain. Kejahatan dilihat sebagai hasil proses-proses dinamika kelas yang memuncak dalam penentuan orang dan perilaku-perilaku tertentu sebagai kejahatan dan penjahat.

2. Definisi-definisi kejahatan terdiri dari perilaku-perilaku yang bertentangan dengan kepentingan kelas dominan

   Perumusan-prumusan kejahatan terdiri dari perilaku-perilaku yang mengalami konflik dengan kepentingan-kepentingan kelas dari kelas ekonomi dominan. Dengan demikian formulasi rumusan kejahatan adalah salah satu manifestasi paling jelas mengenai adanya konflik kelas dalam masyarakat. Kemungkinan perumusan kejahatan akan diformulasikan bertambah dengan adanya faktor-faktor berubahnya struktur sosial, bangkitnya kepentingan-kepentingan kelas dan peningkatan perhatian untuk melindungi kepentingan-kepentingan kelas.

3. Definisi-definisi kejahatan diterapkan oleh kelas yang mempunyai kekuasaan untuk menegakkan dan melaksanakan hukum pidana

   Perumusan kejahatan diterapkan oleh kelas yang mempunyai kekuasaan dalam menegakkan dan melaksanakan hukum pidana. Keungkinan rumusan-rumusan kejahatan dapat diterapkan, dipengaruhi oleh faktor-faktor komuniti dan organisasional seperti harapan-harapan masyarakat terhadap penegakan

dan pelaksanaan hukum, kejelasan dan laporan masyarakat mengenai kejahatan dan organisasi tugas, ideologi dan tindakan-tindakan hamba hukum yang mendelegasikan wewenang untuk menegakkan dan melaksanakan hukum pidana.

4. Pola-pola perilaku dibangun dalam hubungannya dengan rumusan-rumusan kejahatan dan dalam konteks ini orang terlibat dalam tindakan-tindakan yang relatif mempunyai kemungkinan untuk dirumuskan sebagai kejahatan.

   Kemungkinan bahwa seseorang mengembangkan pola-pola tindakan yang mempunyai potensi tinggi untuk dirumuskan sebagai penjahat tergantung pada substansi relatif dari struktur-struktur, pengalaman dalam proses belajar, identifikasi-identifikasi dan persekutuan-persekutuan antar pribadi dan konsep diri,

5. Ideologi tentang kejahatan dibentuk dan disebarluaskan oleh kelas dominan untuk memelihara hegemoninya melalui komunikasi

6. Realitas sosial kejahatan dibentuk oleh perumusan dan penerapan definisi-definisi kejahatan, perkembangan pola-pola perilaku dalam kaitannya dengan definisi ini dan terbentuknya konsepsi-konsepsi kejahatan. Teori realitas sosial kejahat dengan demikian mengandaikan adanya penciptaan seperangkat gejala yang meningkatkan kemungkinan kejahatan dalam masyarakat.

Realitas sosial dapat diartikan sebagai kenyataan tentang kejadian-kejadian atau disebut juga realitas tentang fenomena dan sebagai gambaran tentang kenyataan atau pengetahuan tentang kenyataan atau disebut juga realitas konseptual. Realitas sosial bukanlah keadaan atau kenyataan yang seakan-akan

jatuh dari langit, akan tetapi keberadaannya karena diadakan atau dikonstruksikan secara sosial. Realitas dapat dipandang sebagai kualitas tentang fenomena yang kita terima sebagai hal yang benar, yang keberadaannya tidak tergantung dari kehendak kita sendiri, artinya dia ada di sana dan tetap di sana meski kita tidak menghendakinya, dan merupakan produk yang dihasilkan oleh pelaku-pelaku sosial, yaitu berdasarkan ideologi dan kepentingan-kepentingan mengarahkan tindakannya pada tujuan-tujuan tertentu.[192]

Realitas sosial yang ada pada manusia tidak ada dengan sendirinya, artinya manusia menciptakan realitas sosial itu sebagai bagian dari dinamika kehidupannya. Manusia menciptakan realitasnya seperti apa yang mampu dilakukan dan diinginkan. Hal ini berbeda dengan binatang. Binatang tidak mampu menciptakan realitasnya sendiri, ia hanya menerima realitas yang dihadapi seperti apa adanya tanpa berusaha untuk mengkonstruksikan realitas seperti yang diinginkan. Kepasrahan yang ada pada binatang menunjukkan bahwa binatang tidak mempunyai kebutuhan untuk menciptakan dunianya sendiri. Hal ini berbeda dengan manusia yang harus menciptakan dunianya sendiri di mana aktivitas itu bukan suatu fenomena non biologis tetapi merupakan konsekuensi langsung dari konstruksi biologis manusia.

Dalam kaitannya dengan realitas sosial kejahatan, maka kejahatan tidaklah ditemukan melainkan dirumuskan atau dikontruksikan oleh mereka yang mempunyai kekuasaan. Kejahatan bukan merupakan suatu fenomena yang perwujudannya mudah diamati karena dia merupakan hasil konstruksi oleh

---

192 I.S. Susanto, *Pemahaman Kritis Terhadap Realitas Sosial*, Makalah pada Lokakarya Pengembangan SDM IMKA di Karangpandan, 12-17 Agustus 1992, hal. 1.

pelaku-pelaku sosial atas suatu aksi atau kejadian yang terjadi dalam konteks tertentu. Untuk memutuskan suatu realitas sosial itu sebagai kejahatan dipengaruhi oleh pengetahuan dan persepsi orang yang terbentuk melalui proses sosial tertentu.

Para konstruksionalis berasumsi bahwa obyek tak berada terpisah dari pikiran kita dan setiap realitas itu memiliki makna apabila realitas itu bisa masuk dalam persepsi kita. Asumsi epistemologinya adalah bahwa pengamatan itu didasarkan pada konstruksi pikiran, bukan pada pemahaman mentah tentang dunia fisik. Konstruksionalis sosial tidak tertarik pada hubungan antara realitas obyektif dan observasi tetapi tertarik pada observasi dan pemanfaatan observasi semacam itu untuk memahami dunia kita yang bersifat subyektif dan bermakna ganda.[193]

Dengan asumsi-asumsi seperti itu konstruk ilmuwan sosial harus didasarkan pada dunia yang diciptakan oleh aktor-aktor sosial. **Alfred Schutz** merumuskan masalahnya sebagai berikut "Konstruk ilmu-ilmu sosial adalah konstruk pada tingkat kedua, yaitu konstruk atas konstruk yang dibuat oleh para pelaku dipentas sosial yang perilakunya harus diamati dan dijelaskan sesuai dengan aturan prosedur disiplin ilmunya". Jadi dunia yang penting bagi konstruksionalis sosial adalah dunia yang diciptakan oleh prilaku sosial manusia, oleh interaksi dengan manusia lain. Realitas sosial ini melibatkan makna sosial dan produk dunia sehari-hari yang bersifat subyektif.[194]

---

[193] Richard Quinney, *Criminology, Analysis and Critique of Crime in America*, Little, Brown and Company (Inc), 1975, hal. 10

[194] *Ibid*

Konstruksionalis telah memberikan vitalitas atau semangat baru pada studi tentang kejahatan. Dengan keluar dari studi-studi positivistik, konstruksionalis telah mengarahkan perhatiannya pada sifat tatan hukum yang bermasalah. Kejahatan dan perilaku lainnya pertama-tama dikaji sebagai kategori yang diciptakan dan dikenakan pada beberapa orang oleh orang lainnya. Kejahatan ada karena masyarakat membangun dan menempelkan kata kejahatan. Hukum pidana juga tidak lepas dari masyarakat, tetapi dia sendiri merupakan sebuah konstruksi yang diciptakan oleh mereka-mereka yang berada di kekuasaan. Pengelolaan keadilan adalah kegiatan sosial manusia yang dibangun ketika pelaku hukum menafsirkan dan memberlakukan tatanan mereka pada orang-orang yang mereka pilih untuk diproses.[195]

Salah satu kegagalan pemikiran konstruksi sosial adalah mereka gagal untuk memberi penilaian apakah suatu realitas memiliki lebih unsur-unsur kebaikan dibanding realitas yang lain. Relativisme sosial mencegah pemahaman yang kritis atas dunia. Untuk mengatasi kegagalan ini maka perlu digunakan pendekatan yang lain yaitu pendektan kritis atas realitas sosial yang terjadi. Metode kritis merupakan metode yang filosofinya sangat radikal, yaitu filosofi yang diarahkan pada akar kehidupan kita, pada fondasi, pada esensi kesadaran.[196]

Dalam menelusuri asumsi-asumsi kita dapat melakukan penilaian pada setiap pengalaman yang aktual dan pengalaman yang mungkin terjadi. Cara bekerja pendekatan ini adalah demistifikasi, menghilangkan mitos-anggapan

---

[195] *Ibid*. hal. 11
[196] *Ibid*. hal. 10-12

yang keliru yang diciptakan oleh realitas formal. Pengalaman konvensional diperhatikan sebagai pengkonkritan dari tatanan sosial, dengan mengekspose atau memperlihatkan apa yang ada dibalik realitas.[197]

Tradisi filsafat klasik memiliki sikap bahwa gagasan berfungsi untuk mengarahkan tindakan bahwa hidup harus diterangi pikiran. Filsafat kritis seperti yang dinyatakan oleh **Habermas** adalah filsafat yang menghancurkan ilusi tentang obyektivitas (yaitu ilusi tentang realitas yang terpisah dari kesadaran). Bila dipandang dengan cara ini, pikiran itu sendiri selalu bersifat kritis. Dalam menghilangkan mitos kehidupan kita, perhatian kita diarahkan untuk mengkritisi kita sekarang ini.[198]

Tanpa pemikiran kritis kita hanya akan terikat dengan kehidupan sosial yang sudah kita kenal yaitu kehidupan yang ada, sehingga kita tidak bebas untuk memilih kehidupan yang lebih baik. Apa yang kita lakukan hanyalah sekedar mendukung sistem yang selama ini melingkupi kita. Budaya dan struktur masyarakat yang ditopang oleh sistem birokrasi dan teknologi dalam produksi dan distribusi merupakan ancaman bagi kebebasan individu, termasuk kebebasan untuk mengetahui bahwa sistem itu tidak sempurna dan bisa diubah. Sistem semacam ini bisa mencegah tumbuhnya oposisi dari dalam. Kita tak dapat mempertimbangkan eksistensi yang lain. Itulah pesan **Marcuse** dalam membahas "karakter berdimensi tunggal dari realitas masa kini kita". Hanya dengan menolak masa kini, kita dapat mengalami sesuatu yang lain.[199]

---

197 *Ibid*
198 *Ibid*
199 *Ibid.*

Pendekatan kritis adalah cara pandang atau kerangka pemikiran yang mengarahkan untuk mempelajari proses-proses yang dilakukan manusia dalam membangun masyarakatnya atau dunianya. Oleh karena itu setiap masyarakat manusia merupakan kegiatan pembangunan dunia maka masyarakat adalah fenomena dialektika, artinya masyarakat adalah produk manusia dan sebaliknya manusia adalah produk masyarakat. Ini berarti tidak ada realitas sosial yang terpisah dari manusia. Melaui pendekatan kritis dapat ditunjukkan proses-proses pembentukan realitas sosial, yaitu proses diterimanya tindakan-tindakan orang menjadi suatu realitas dihubungkan dengan kondisi-kondisi struktur, politik, sosial, ekonomi dan budaya yang ada.[200]

Proses fundamental dari dialektika masyarakat itu menurut **Peter L. Berger** dan **Thomas Luckmann** terdiri dari tiga peristiwa, yaitu eksternalisasi, obyektivasi dan internalisasi. *Eksternalisasi* adalah suatu pencurahan kedirian manusia secara terus menerus ke dalam dunia, baik dalam aktivitas fisis maupun mentalnya. *Obyektivasi* adalah disandangnya produk-produk aktivitas itu (baik fisis maupun mental) suatu realitas yang berhadapan dengan para produsennya semula, dalam bentuk suatu kefaktaan (faktisitas) yang eksternal terhadap dan lain dari para produser itu sendiri. *Internalisasi* adalah peresapan kembali realitas tersebut oleh manusia dan mentransformasikan sekali lagi dari struktur-struktur dunia obyektif ke dalam struktur-struktur kesadaran subyektif.[201]

---

[200] I.S. Susanto, *op.cit*, hal. 3-4

[201] Uraian lebih lengkap mengenai persoalan eksternalisasi, obyektivasi dan internalisasi dalam kaitannya dengan masyarakat sebagai kenyataan obyektif yang mempermasalahkan hubungan manusia dengan lingkungannya sehingga dicapai kesimpulan masyarakat merupakan produk manusia, masyarakat merupakan kenyataan obyektif dan manusia merupakan produk sosial serta masyarakat sebagai kenyataan subyektif sebagai rangkaian proses dialektika berupa internalisasi. Hal tersebut dapat dijumpai dalam karya Peter L. Berger dan Thomas Luckman, *Tafsir Sosial Atas Kenyataan, Risalah tentang Sosiologi Pengetahuan*, LP3ES, Jakarta, 1990. Lihat juga penjelasan lebih lanjut dalam karya Peter L. Berger, *Langit Suci, Agama Sebagai Realitas Sosial*, LP3ES, Jakarta, 1994

Manusia adalah pencipta kenyataan sosial yang obyektif melalui proses eksternalisasi, sebagaimana kenyataan obyektif mempengaruhi kembali manusia melalui proses internalisasi (yang mencerminkan kenyataan subyektif). Dengan kemampuan berfikir dialektis ini, **Berger** memandang masyarakat sebagai produk manusia dan manusia sebagai produk masyarakat. Salah satu tugas pokok sosiologi pengetahuan adalah menjelaskan dialektika antar diri dengan dunia sosio kultural. Dialektika itu berlangsung dalam suatu proses dengan tiga momen simultan, yakni *eksternalisasi* (penyesuaian diri dengan dunia sosio-kultural sebagai produk manusia), *obyektivasi* (interaksi sosial dalam dunia intersubyektif yang dilembagakan atau mengalami proses institusionalisasi) dan *internalisasi* (individu mengidentifikasikan diri dengan lembaga-lembaga sosial atau organisasi sosial tempat individu menjadi anggotanya. Dengan memandang masyarakat sebagai proses yang berlangsung dalam tiga momen dialektis yang simultan itu (ditambah dengan masalah legitimasi yang berdimensi kognitif dan normatif) maka kenyataan atau realitas sosial itu merupakan konstruksi sosial buatan masyarakat sendiri dalam perjalanan sejarahnya dari masa silam ke masa kini dan menuju masa yang akan datang.[202]

Realitas sosial kejahatan dikonstruksikan oleh formulasi dan penterapan batasan-batasan dari kejahatan, perkembangan perikelakuan yang berkaitan dengan batasan-batasan tentang kejahatan dan konstruksi daripaka konsepsi-konsepsi kriminal. Realitas sosial merupakan dunia yang diciptakan manusia, dunia mana merupakan miliknya. Realitas tersebut terbentuk melalui pengetahuan yang diperkembangkan oleh manusia, cita-cita yang dikandungnya

---

[202] *Ibid*

dan perikelakuannya. Manusia juga memperkembangkan konsepsi-kosepsi mengenai apa yang dianggapnya sebagai kejahatan di dalam kerangka realitas sosial tersebut. Penciptaan konsepsi-konsepsi tersebut terjadi melalui interaksi sosial yang berintikan pada syarat-syarat adanya kontak sosial dan komunikasi.[203]

2. Pendekatan Interaksionisme Simbolik dalam Kriminologi Kritis

Pembentukan realitas sosial selain ditentukan oleh pengetahuan yang dimiliki oleh pelaku atau aktor yang terlibat di dalamnya, juga ditentukan oleh proses komunikasi atau interaksi yang terjadi antara pelaku atau aktor yang satu dengan yang lainnya. Berkaitan dengan proses-proses komunikasi dan interaksi itu maka perlu dikemukakan perspektif interaksionisme simbolik dalam pembentukan realitas sosial. Interaksionisme simbolik sebagai salah satu aliran utama dalam sosiologi sangat berpengaruh dalam pengembangan dan perkembangan pemikiran kriminologi kritis terutama teori realitas sosial kejahatan dan teori labeling.

Pendekatan interaksionis dalam kriminologi kritis berusaha untuk menentukan mengapa tindakan-tindakan dan orang-orang tertentu didefinisikan sebagai kriminal di masyarakat tertentu dengan cara mempelajari persepsi makna kejahatan yang dimiliki oleh masyarakat yang bersangkutan. Mereka mempelajari makna kejahatan yang dimiliki oleh agen kontrol sosial dan orang-orang yang diberi batasan sebagai penjahat, juga mempelajari makna proses sosial yang dimiliki kelompok yang bersangkutan dalam mendefinisikan seseorang sebagai penjahat. Teori interaksionis menolak pendapat kaum

---

[203] Soerjono Soekanto dkk, *op.cit*, hal. 29

positivis yang mengatakan bahwa pelaku kejahatan adalah suatu tipe manusia yang unik yang diciptakan atau dibentuk oleh hubungan sebab akibat yang unik pula. Teori interaksionis ini menitikberatkan pada relativitas tingkah laku kriminal.

Hubungan antara kejahatan dan proses kriminalisasi secara umum dinyatakan sengan digunakannya konsep penyimpangan (*deviance*) dan reaksi sosial. Kejahatan dipandang sebagai bagian dari penyimpangan sosial dan tindakan tersebut berbeda dari tindakan-tindakan yang dipandang sebagai normal atau biasa di masyarakat. Tindakan menyimpang itu diberikan reaksi sosial yang negatif dalam arti secara umum masyarakat memperlakukan orang-orang tersebut sebagai berbeda dan jahat. Dasar pemikiran interaksionis ini bersumber pada *symbolic interactionism* yang dikemukakan oleh **George Herbert Mead,** yang menekankan bahwa sumber perilaku manusia tidak hanya ditentukan oleh peranan kondisi-kondisi sosial akan tetapi juga peranan individu dalam menangani, menafsirkan dan berinteraksi dengan kondisi-kondisi yang bersangkutan. Manusia merupakan pencipta dan sekaligus sebagai produk dari lingkungannya.[204]

Dalam analisanya, interaksionisme simbolik melihat realitas sosial sebagai proses daripada sebagai sesuatu yang statis. Manusia bukan dilihat sebagai produk yang ditentukan oleh struktur atau situasi obyektif, tetapi paling tidak sebagaian merupakan aktor-aktor yang bebas. Fakta-fakta obyektif memang penting tetapi tidak berarti fakta subyektif diabaikan. Berkaitan dengan fakta subyektif ini **Charles H. Cooley** berpendapat bahwa imajinasi yang

---

[204] *Ibid.* hal. 9-10

dimiliki manusia merupakan fakta masyarakat yang solid dan berfungsi sebagai suatu warisan realitas dunia subyektif. Hal senada juga diungkapkan oleh **William Isaac Thomas**.

Jika **Cooley** dan **Thomas** melihat masalah pokok dalam interaksionisme simbolik berupa "imajinasi-imajinasi", **Mead** justru melihat bagaimana proses individu menjadi anggota organisasi yang disebut masyarakat sebagai masalah yang rumit. Dalam model dialektika **Berger**, permasalahan yang dikemukakan **Mead** termasuk dalam persoalan internalisasi. Dijelaskan oleh **Mead** bahwa diri atau *self* menjalani internalisasi atau interpretasi subyektif atas realitas (obyektif) struktur yang lebih luas. Diri atau *self* itu benar-benar merupakan internalisasi seseorang atas apa yang telah digeneralisir orang lain atau kebiasaan-kebiasaan sosial komunitas yang lebih luas. Dia merupakan produk dialektis dari "saya" atau impulsif dari diri, dan "aku", atau sisi sosial manusia. Karena itu setiap diri seseorang terdiri dari biologis dan psikologis "saya" dan sosiologis "aku".[205]

Dalam hal ini **Cooley** mengajukan dua konsep. Pertama konsep yang dinamakan *the concept of self*. *Self* dilihat oleh **Cooley** sebagai suatu proses di

---

[205] Margaret M. Poloma, *Sosiologi Kontemporer*, diterbitkan atas kerjasama PT. RajaGarfindo Persada Jakarta dan Yayasan Solidaritas Gadjah Mada Yogyakarta, 1994, hal. 259-260. Konsep diri dalam hal ini ditunjukkan oleh Mead dalam hubungan timbal balik antara diri sebagai obyek dan diri sebagai subyek. Diri sebagai obyek ditunjuk dengan konsep "me", diri sebagai subyek yang bertindak ditunjuknya dengan konsep "I" yang merupakan aspek diri yang bersifat non-reflektif. Dia tidak mencakup ingatan-ingatan dari tindakan masa lampau atau antisipasi masa di masa yang akan datang. Dia merupakan respon perilaku aktual dari individu pada momen eksistensinya sekarang ini terhadap tuntutan situasi yang berhubungan dengan kebutuhan-kebutuhan atau rencana-rencana sekarang ini. Hubungan antara I dan me itu bersifat saling tergantung secara dinamis. Cooley menamakan konsep diri ini dengan istilah *looking-glass self*, artinya setiap hubungan sosial di mana seseorang itu terlibat merupakan suatu cerminan diri yang disatukan dalam identitas orang itu sendiri. Orang dapat dibayangkan sebagai hidup dalam suatu dunia cermin, yang masing-masing memberi perspektif atau seginya sendiri yang khusus. Cermin akan memberikan pantual yang bias atau suram atau jernih tergantung pada tindakannya. Doyle Paul Johnson, *Teori Sosiologi Klasik dan Modern*, Gramedia, Jakarta, 1986, hal. 18 dan 28

mana para individu melihat diri mereka sebagai obyek, bersama-sama dengan obyek lain dalam lingkungan sosial mereka. Kedua **Cooley** mengakaui bahwa munculnya *self* karena berkomunikasi dengan orang-orang lain. Dalam konteks ini **Cooley** lalu menamakan proses interaksi ini, juga dalam berkelompok sebagai suatu proses *the looking glass self.*

Mead tidak hanya menyadari orang lain tetapi juga mampu menyadari dirinya sendiri, orang tidak hanya berinteraksi dengan orang lain tetapi secara simbolis dia juga berinteraksi dengan dirinya sendiri. Interaksi simbol dilakukan dengan menggunakan bahasa sebagai satu-satunya simbol yang terpenting dan melalui isyarat (*people interact with one another largely via symbol - images, sounds, smells, etc., which symbolise, that is stand for, other things*). Simbol bukan merupakan fakta-fakta yang sudah jadi, simbol berada dalam proses yang kontinyu. Proses penyampaian makna inilah yang merupakan subject matter dari sejumlah analisa kaum interaksionisme simbolis. Dalam pandangan **Herbert Blumer**, interaksionisme simbolis bertumpu pada tiga premis, yaitu:[206]

1. Manusia bertindak terhadap sesuatu berdasarkan makna-makna yang ada pada sesuatu itu bagi mereka.
2. Makna tersebut berasal dari interaksi sosial seseorang dengan orang lain

---

[206] Herbert Blumer, Symbolic Interactionism: Perspective and Method, 1969 sebagaimana dikutip oleh Margaret M. Poloma, *Ibid*, hal. 261. Pikiran atau kesadaran muncul dari proses penggunaan simbol secara tak kelihatan, khususnya simbol-simbol bahasa, atau dengan kata lain pikiran adalah proses penggunaan simbol internal atau yang bersifat tidak kelihatan. Suatu segi yang penting dari model ini tentang intelegensi manusia dalah bahwa dia mencakup kesadaran tentang diri (*self-consciousness*). Manusia memikirkan tindakan-tindakan yang potensial lebih dulu dari pelaksanaannya dan menilainya menurut konsekuensi-konsekuensi yang dibayangkan terlebih dahulu, termasuk reaksi-reaksi yang mungkin muncul dari orang lain. Hal ini menuntut mereka untuk menjadi obyek bagi mereka sendiri (yaitu kesadaran tentang diri atau reflektif). Doyle Paul Johnson, *op.cit*, hal. 15-16

3. Makna-makna tersebut disempurnakan di saat proses interaksi sosial berlangsung.

Tindakan manusia bukan disebabkan oleh beberapa kekuatan luar, tidak pula disebabkan oleh kekuatan dalam. Gambaran yang benar ialah manusia membentuk obyek-obyek, individu sebenarnya sedang merancang obyek-obyek yang berbeda, memberi arti, menilai kesesuaiannya dengan tindakan dan mengambil keputusan berdasarkan penilaian tersebut. Inilah yang oleh **Blumer** dimaksud dengan penafsiran atau bertindak berdasarkan simbol-simbol. Dengan demikian manusia merupakan aktor yang sadar dan reflektif, yang menyatukan obyek-obyek yang diketahuinya menjadi apa yang disebut oleh **Blumer** sebagai proses *self indication. Self indication* adalah proses komunikasi yang sedang berjalan di mana individu mengetahui sesuatu, menilainya, memberinya makna dan memutuskan untuk bertindak berdasarkan makna itu. Proses *self indication* ini terjadi dalam konteks sosial di mana individu mencoba mengantisipasi tindakan-tindakan orang lain dan menyesuaikan tindakannya sebagaimana dia menafsirkan tindakan itu.[207]

Menurut **Blumer**, masyarakat merupakan hasil interaksi simbolis dan aspek inilah yang harus merupakan masalah bagi para sosiolog. Keistimewaan pendekatan interaksionis simbolis ialah manusia dilihat saling menafsirkan atau membatasi masing-masing tindakan mereka dan bukan hanya bereaksi kepada setiap tindakan itu menurut mode stimulus-respon. Seseorang tidak langsung

---

[207] *Ibid*, hal. 264.

memberikan respon pada tindakan orang lain, tetapi didasarkan pada pengertian yang diberikan kepada tindakan itu. Dengan demikian interaksi manusia dijembatani oleh penggunaan simbol-simbol, oleh penafsiran, oleh kepastian makna dari tindakan-tindakan orang lain.[208]

Interaksionisme-simbolis yang diketengahkan oleh **Blumer** mengandung sejumlah *root images* atau ide-ide dasar yang dapat diringkas sebagai berikut:[209]

1. Masyarakat terdiri dari manusia yang berinteraksi. Kegiatan tersebut saling bersesuaian melalui tindakan bersama, membentuk apa yang dikenal sebagai organisasi atau struktur sosial.
2. Interaksi terdiri dari berbagai kegiatan manusia yang berhubungan dengan kegiatan manusia lain
3. Obyek-obyek tidak mempunyai makna yang intrinsik, makna lebih merupakan produk interaksi simbolis

---

208 *Ibid*, hal. 266. Bandingkan dengan pendapat Watson yang memusatkan perhatiannya pada perilaku nyata (overt behaviour) atau proses-proses psikologis yang dapat diukur. Perilaku dijelaskan menurut gerak-gerak refleks yang dipelajari atau yang sudah menjadi kebiasaan, rangsangan atau proses psikologis yang dapat diukur secara empiris. Hal ini ditentang oleh Mead yang memperlihatkan bahwa model Watson hanya berupa stimulus-response atau gerak-gerak refleks yang dipelajari tidak lengkap karena pikiran atau kesadaran muncul dalam tindakan karena adanya persepsi tentang dunia luar, proses-proses fisiologis dan kesadaran subyektif yang semuanya saling tergantung. Individu-individu tidak bertindak sebagai organisme yang terasing, tindakan-tindakan mereka saling berhubungan dan saling tergantung. Proses komunikasi dan interaksi di mana individu-individu saling mempengaruhi, saling menyesuaikan diri atau di mana tindakan-tindakan individu saling cocok, tidak beda secara kualitatif dari proses berfikir internal. Doyle Paul Johnson, *op.cit*, hal. 9-10

209 *Ibid*, hal. 267-268. Bandingkan dengan Goode yang mengemukakan tiga kunci pangkal tolak untuk para interaksionis, yaitu:
1. Orang beraksi berdasarkan makna (meanings)
2. Makna timbul karena adanya interaksi dengan orang lain terutama dengan orang yang sangat dekat (intimate others)
3. Makna terus menerus berubah karena adanya interpretasi terhadap obyek, orang lain dan situasi

4. Manusia tidak hanya mengenal obyek eksternal, mereka dapat melihat dirinya sebagai obyek
5. Tindakan manusia adalah tindakan interpretatif yang dibuat oleh manusia itu sendiri
6. Tindakan tersebut saling dikaitkan dan disesuaikan oleh anggota-anggota kelompok, hal ini disebut sebagai tindakan bersama yang dibatasi sebagai organisasi sosial dari perilaku tindakan-tindakan berbagai manusia.

Dalam konteks pembicaraan mengenai interaksi ini perlulah dikemukakan pendapat **Emile Durkheim**. Dalam bukunya *Division of Labor in Society*, **Durkheim** menggambarkan realitas sosial sebagai *"... as an emergent phenomena, sui generis, and as not reducible to the psychic states of individual"*. **Durkheim** mengajukan beberapa pertanyaan bagaimana masyarakat mengatur individu, bagaimana masyarakat menguasai individu dan membina mereka tidak dari luar serta mengapa orang-orang menganut orientasi dan perspektif yang sama. **Weber** sendiri mengakui adanya realitas di belakang struktur sosial yang makro, yang merupakan interaksi simbolik yang bermakna antara manusia.[210]

Pentingnya reaksi sosial terhadap konsep diri seseorang dapat dilihat dalam studi-studi mengenai penyimpangan. Perspektif interaksionisme simbol mengenai penyimpangan memulai dengan suatu pengakuan bahwa penyimpangan tidak hanya sekadar suatu manifestasi suatu ciri pembawaan sejak lahir atau cacat kepribadian seperti yang menjadi fokus bahasan kriminologi positif. Dalam perspektif interaksionisme simbol penyimpangan dihasilkan sebagai akibat dari suatu tipe proses interaksi tertentu.

---

[210] J.E. Sahetapy, *op.cit*, hal. 3-4

Penyimpangan selalu didefinisikan dalam hubungannya dengan standar-standar normatif tertentu dalam suatu masyarakat atau kelompok. Definisi mengenai apa itu penyimpangana atau apa itu konformitas, akan berbeda-beda untuk masyarakat yang berbeda-beda atau kelompok yang berbeda-beda dalam suatu masyarakat. Hal ini disebabkan karena manusia dalam menilai sesuatu tidak hanya berdasarkan kesadaran obyektif (seperti yang ditentukan dalam standar-standar normatif) tetapi juga didasarkan pada penilaian subyektif berupa interpretasi terhadap kenyataan.

Standar-standar normatif dan peraturan-peraturan dalam suatu kelompok atau masyarakat biasanya bersifat umum dan harus diinterpretasi supaya dapat diterapkan pada situasi-situasi tertentu, jadi selalu ada kemungkinan setiap individu bisa berbeda dalam interpretasinya mengenai apakah pola-pola normatif itu sudah secukupnya diikuti dalam suatu situasi tertentu. Interpretasi ini merupakan hasil dari proses berfikir yang dimulai atau dirangsang oleh munculnya suatu masalah atau hambatan yang menghalangi tindakan-tindakan individu untuk memenuhi kebutuhannya. Individu mungkin berfikir melalui serangkaian pemecahan yang bersifat alternatif dan berusaha untuk menilai konsekuensi-konsekuensi yang mungkin terjadi sebelum menentukan satu yang akhir dan mudah-mudahan memuaskan.

Pola-pola normatif bersama atau harapan-harapan orang lain mungkin tidak konsisten dengan dorongan hati atau kepentingan kita, artinya orang lain mungkin mengharapkan supaya kita mengikuti pola-pola normatif tertentu dalam situasi di mana kita tidak merasa enak untuk berbuat demikian. Melihat perbedaan-perbedaan dalam interpretasi mengenai pola-pola normatif dan

ketegangan yang tering terjadi antara tuntutan normatif dan kepentingan dan keinginan individu, banyak orang mungkin sesekali menyimpang dari norma-norma itu. Penyimpangan itu terkadang tidak membawa dampak yang besar atau dianggap sepi karena tidak menimbulkan akibat yang berpengaruh pada orang lain, tetapi sebaliknya dapat terjadi penyimpangan itu dapat menimbulkan reaksi dari aparat atau petugas hukum karena dianggap sudah menganggu ketentraman dan kenyamanan hidup bermasyarakat. Perilaku menyimpang merupakan sifat pokok dalam interaksi dan akhirnya merupakan elemen utama dalam identitas-diri si penyimpang.

Proses hukum dalam proses peradilan pidana terhadap si penyimpang biasanya akan berpengaruh sekali terhadap cara orang lain menerima dan memperlakukan orang itu karena sebelum pengadilan menjatuhkan putusan, si penyimpang atau tersangka itu sudah dianggap bersalah meskipun sebetulnya ada asas *presumption of innocence* atau asas praduga tidak bersalah. Sebagai akibatnya individu itu akan cenderung mengembangkan suatu identitas diri sebagai seorang penyimpang atau kriminal dan sikapnya terhadap masyarakat dan orang lain akan mencerminkan suatu tingkah permusuhan tertentu atau alienasi.

Teori interaksionis simbolik yang berkaitan dengan kejahatan ini berlandaskan pada pemikiran:[211]

1. Kejahatan adalah merupakan kualitas daripada reaksi/tanggapan terhadap tingkah laku, bukan merupakan kualitas dari sesuatu tingkah laku
2. Tingkah laku yang relatif tersebut telah memberikan cap sebagai penjahat

---

[211] Romli Atmasasmita, *Bunga Rampai ... op.cit*, hal. 102.

3. Tingkah laku seseorang yang dicap jahat juga diberi atau diperlakukan sebagai penjahat
4. Seseorang diberi cap atau diperlakukan sebagai penjahat melalui suatu proses interaksi
5. Terhadap suatu kecenderungan di mana seseorang yang dicap sebagai penjahat akan bertingkah laku sebagaimana perlakuan atau cap itu diberikan.

Orang-orang yang dipisahkan atau diperlakukan seperti itu akan bersatu dan membentuk serta mengembangkan sub kutlturnya yang mencerminkan usaha untuk menyesuaikan diri dengan penolakan masyrakat dan memenuhi kebutuhan mereka sendiri, baik yang bersifat konvensional maupun yang bersifat menyimpang. Dengan cara ini identitas mereka muncul dari proses interaksi dan secara bertahap mengambil dan menyesuaikan diri dengan identitas-identitas penyimpangan seperti yang dicapkan kepada mereka oleh wakil-wakil masyarakat.

Dengan demikian masyarakatlah yang menciptakan orang-orang yang menyimpang dengan membuat peraturan-peraturan yang pelanggarannya menimbulkan penyimpangan dan memperlakukan secara khusus pelanggarnya itu. Kepentingan masyarakat yang bersifat normatif secara politik adalah kuat atau kalau tidak memiliki tingkat yang tinggi dalam keseluruhan sistem stratifikasi sosial sehingga dapat mempengaruhi bentuk-bentuk penyimpangan yang dapat dikenai sanksi.

Mereka yang mempunyai kekuasaan politik dan ekonomi mungkin berperilaku menurut cara yang merugikan banyak kelompok lain tetapi mereka dengan kekuasaannya menghindari untuk dianggap atau dihukum sebagai

penyimpang. Kriteria yang digunakan untuk menentukan bentuk-bentuk penyimpangan tertentu mencerminkan suatu proses sosial yang kompleks yang didasarkan pada definisi-definisi subyektif dan pada penyebaran sumber-sumber yang menimbulkan perbedaan yang memungkinkan kelompok-kelompok tertentu (terutama kelompok yang secara politis dan ekonomis lebih superior) untuk memaksakan definisinya sendiri pada kelompok lain (yang secara politis dan ekonomis lebih *inferior* sehingga tidak mempunyai kekuatan untuk mempengaruhi)

Para teoritisi interaksionis sering dinamakan teoritisi anti-positivis atau *labeling orientation* atau *interactionist theory of deviance*. Istilah-istilah menurut **Gwynn Nettler** mengindikasikan *"... the causal power of response - verbal and nonverbal - to classes of people and classes of acts"*, karena mereka memahamai permasalahan kejahatan tidak secara absolut. Dengan kata lain pemahaman para teoritisi interaksionis berkutat dengan pemahaman secara relatif.[212]

Tidak ada suatu teori tanpa kritik. Teori interaksionisme simbolik ini juga tidak luput dari kritik. **Jack Gibbs** berpendapat ada dua kelemahan teori interaksionis. Pertama dikatakan oleh **Gibbs** bahwa *relativistic in the extreme, interactionism offers no causal analysis of the factors that precitipitate acts of deviance*. Jadi teoriinteraksionis tidak mengidentifikasi kausa, melainkan lebih suka memberi pumpungan kepada reaksi sosial terhadap perilaku itu, seperti perilaku perkosaan, homoseksual dan sebagainya. Kedua, *"... interactionist analysis ignore the exsistence of widely accepted norms whose infringement is*

---

[212] *Ibid*, hal. 3.

indeed deviant". Sebagai contoh apabila ada orang berjalan telanjang bulan di jalan umum dan yang lain tidak apakah untuk perilaku yang pertama masih harus menunggu sampai ada reaksi sosial?[213]

Kritik ini ditanggapi oleh **Suchar** dengan argumen sebagai berikut:

> Interactionists do no concern themselves with the ultimate precipitates of deviance ... this does not mean that (they offer) an invalid perpective on deviance. Rather than deny the possibility of understanding the ultimate precipitates of deviant behaviour, most interactionists believe that it is more important to examine those processes that make deviation the socially meaningfull reality that it is.[214]

Selain kritik di atas ada yang berpendapat bahwa tidak ada cukup bukti untuk mendukung pendapat teori interaksionis. **Charles Tittle** berpendapat bahwa kurang ada makna dari reaksi sosial terhadap deviasi primer, di samping itu masih ada kritik lain yang mengemukakan bahwa teori interaksionis mengabaikan hubungan antara perbuatan devian dan struktur sosial sebagai suatu keseluruhan. Terhadap hal tersebut **Ian Taylor, Paul Walton** dan **Jock Young** mengemukakan bahwa para interaksionis cuma memperhatikan apa yang dinamakan *small-scale_interacions dan sama sekali mengabaikan "... wider origins of deviant acts and of social reaction of these"*[215]

Terlepas dari berbagai kritik itu, teori interaksionis simbolik memberikan sumbangan terhadap pemikiran baru yaitu teori labeling, yaitu teori yang mendasarkan pada identitas-identitas penyimpangan yang oleh capkan atau dilabelkan oleh wakil-wakil masyarakat terhadap si penyimpang. Teori labeling juga disebut dengan istilah *underdog philosophy* karena memperjuangkan kaum

---

213 Jack Gibbs sebagaimana dikutip oleh J.E. Sahetapy, *ibid.* hal. 11-12
214 Suchar sebagaimana dikutip oleh J.E. Sahetapy, *ibid,* hal. 12
215 Ian Taylor, Paul Walton dan Jock Young, *op.cit*, hal. 273-274

minoritas atau kaum kecil atau mereka yang berada di lapisan bahwa masyarakat.

Teori labeling dapat juga dikatakan merupakan anak dari *symbolic interactionism* dan dalam konteks kriminologi radikal **Scheff** mengemukakan "... *labeling proponents prefer to jostie the imagination, to create a crisis of consciousness which will lead to new visions of reality.* Dengan demikian gagasannya lebih bersifat provokatif daripada empirik yang berarti mereka menghindari kenyataan empirik dan proposisi mereka menjadi licin seperti belut.[216]

Teori labeling memiliki perbedaan orientasi dengan teori yang lain karena penjahat dipandang sebagai orang yang terpisah dari masyarakat luas yang terdiri dari orang-orang yang jujur (atau berpura-pura jujur) dan warga yang patuh (atau berpura-pura patuh). Penjahat merupakan penyakit masyarakat dan dianggap sebagai hasil dari berbagai ciri khusus individu baik biologi atau sosialnya sehingga harus diasingkan atau dijauhi dalam pergaulan masyarakat. Penjahat seolah-olah menjadi manusia atau suku (jika mereka membentuk sub kulturnya sendiri) terasing dalam suatu masyarakat yang baik-baik (atau pura-pura baik untuk menutupi kejahatannya).

Jika teori lain melakukan pendekatan statistik, patologis atau pandangan yang bersifat relatif dalam memahami kejahatan, maka menurut **Howard Becker** (salah seorang pengemuka teori labeling) dianggapnya pendekatan-pendektan tersebut kurang adil dan tidak realistik. Pandangan yang

---

[216] J.E. Sahetapy, *op.cit*, hal. 26

melihat kejahatan dari sudut statistik, patologis dan pandangan relatif lainnya menyebabkan para penggiat atau penstudi di bidang kriminologi hanya menekankan pada usaha-usaha perbaikan terhadap pelaku penyimpangan atau kejahatan dengan melakukan usaha-usaha untuk menarik mereka yang menyimpang itu untuk kembali ke jalan yang lurus. **Becker** melihat kejahatan sering tergantung dari penglihatan si pengamat karena anggota-anggota kelompok yang berbeda memiliki perbedaan konsep tentang apa yang disebut baik dan layak dalam situasi tertentu sehingga menurut **I.S. Susanto** hampir tidak ada perhatian atau tidak pernah disuarakan tentang peranan masyarakat luas dalam mengidentifikasikan atau memproses kejahatan.[217]

Frank Tannembaum, seorang kriminolog yang sering dihubung-hubungkan dengan teori labeling mengungkapkan bahwa kejahatan tidaklah sepenuhnya merupakan hasil dari ketidakmampuan seseorang untuk menyesuaikan dirinya dengan kelompok, akan tetapi dalam kenyataannya ia telah dipaksa untuk menyesuaikan dirinya dengan kelompoknya. Dengan demikian kejahatan merupakan hasil konflik antara kelompok dengan masyarakat yang lebih luas, di mana terdapat dua definisi yang bertentangan tentang tingkah laku yang layak.[218]

Pembahasan mengenai teori ini dimulai dengan melakukan eksplorasi bagaimana dan mengapa suatu perbuatan atau perilaku tertentu didefinisikan sebagai penjahat atau penyimpang dan mengapa perilaku lain tidak didefinisikan demikian. Mereka mempertanyakan bagaimana dan mengapa orang tertentu

---

[217] I.S. Susanto, *Kriminologi*, *op.cit*, hal. 76
[218] Romli Atmasasmita, *op.cit*, hal, 38

kemudian didefinisikan sebagai penjahat atau penyimpang. Beberapa teoritisi labeling berpandangan bahwa penjahat bukan orang yang jahat atau salah perilakunya tetapi sebagai individu yang oleh sistem peradilan pidana dan sebagaian besar masyarakat ditempatkan sebagai orang yang mempunyai status jahat sebagaimana diungkapkan oleh **Howard Beckers**:

> Deviance is not a quality of the act the person commits, but rather a consequence of the application by others of rules and sanctions to an offender. The deviant is one to whom that label has successfully been applied; deviant behavior is behavior that people so label.[219]

Fokus teori labeling pada reaksi orang lain dan berikutnya efek reaksi dari perbuatan yang dilakukan oleh penyimpang (*deviance*). Ketika reaksi itu menjadi pengetahuan bahwa seseorang telah melakukan perbuatan menyimpang, si penyimpang kemudian dipisahkan dari masyarakat dan diberi label sebagai pelacur, pencuri, penyiksa, penghianat, pemadat, pecandu dan sejenisnya. Becker mencatat proses pemisahan ini dinamakan outsiders, yang diusir atau diasingkan dari masyarakat. Orang-orang yang disebut outsiders itu kemudian mulai membentuk asosiasi atau perkumpulan dengan orang lain yang juga menjadi orang yang diusir/buangan.

Pembicaraan mengenai teori labeling ini dapat dibedakan menjadi dua bagian, yaitu:[220]

1. Persoalan tentang bagaimana dan mengapa seseorang memperoleh cap atau label.

   Persoalan ini berkaitan dengan memperlakukan labeling sebagai dependent variable atau variabel tidak bebas dan keberadaannya memerlukan

---

[219] Howard Becker, *Outsiders, Studies in the Sociology of Deviance*, The Free Press, New York, 1963

[220] Pertanyaan-pertanyaan ini terdapat dalam Romli Atmasasmita, *op.cit*, hal, 38

penjelasan. Persoalan ini berkaitan dengan pendapat **Howard Becker** yang menyatakan

> *"social groups create deviance by making the rules whose infraction constitutes deviance, and by applying those rules to particular people and labeling them as outsiders. From this point of view, deviance is not a quality of the act the person commits, but rather a consequence of the application by others of rules and sacntions to an "offender." The deviant is one to whom that label has successfully been applied; deviant behavior is behavior that people so label.*[221]

Jadi dari pernyataan **Becker** itu ada dua dalil yang dikemukakannya dalam teorinya, yaitu:

a. kelompok sosial menciptakan penyimpangan dengan membuat peraturan, bahwa barang siapa melanggarnya akan menghasilkan penyimpangan, dan
b. perilaku menyimpang adalah perilaku yang oleh orang-orang diberi cap demikian.

Ini berarti teori labeling mempermasalahkan peranan orang lain (reaksi), khususnya polisi (dan aparat penegak hukum lainnya) dalam menciptakan kejahatan yang di waktu-waktu sebelumnya tidak atau hampir tidak pernah dipertanyakan. Dengan demikian teori labeling telah mengubah konteks studi kriminologi, yaitu dari penjahat kepada mempelajari proses-proses terjadinya kejahatan atau penjahat dan akibat selanjutnya adalah meningkatnya perhatian dan studi terhadap bekerjanya aparat penegak hukum pada umumnya dan khususnya polisi (dan aparat penegak hukum lainnya). [222]

2. Efek labeling terhadap penyimpangan tingkah laku berikutnya.

---

[221] Howard Becker, *op.cit*, hal. 9
[222] Lihat I.S. Susanto, Kriminologi, *op.cit*, hal. 76

Persoalan ini memperlakukan labeling sebagai variabel yang independen atau variabel bebas atau mempengaruhi yaitu bagaimana labeling mempengaruhi seseorang yang terkena label atau cap. Dalam kaitan dengan hal ini ada dua proses bagaimana labeling memperngaruhi seseorang yang terkena label atau cap untuk melakukan penyimpangan tingkah laku, yaitu:

a. cap atau label tersebut menarik perhatian pengamat dan mengakibatkan pengamat selalu memperhatikannya dan kemudian seterusnya cap atau label tersebut melekat pada diri orang itu
b. cap atau label tersebut sudah diadopsi oleh seseorang dan membawa pengaruh pada dirinya sehingga ia mengakui dengan sendirinya sebagaimana cap atau label itu diberikan padanya oleh si pengamat.

Cap atau label yang diberikan kepada pelaku kejahatan atau penyimpangan akan berpengaruh terhadap orang tersebut, bukan saja pada tingkah laku dalam pergaulan masyarakat tetapi juga usaha-usahanya untuk memperbaiki perilakunya. Kesulitan untuk memperoleh dukungan dari masyarakat dalam memperbaiki perilakunya dan kewaspadaan masyarakat terhadap tingkah laku penyimpang atau penyimpang itu semakin memperkuat penyimpang untuk membentuk karir kriminalnya semakin kuat.

Schrag menyimpulkan asumsi dasar teori labeling ini, yaitu:[223]

1. Tidak ada satu perbuatan yang terjadi dengan sendirinya bersifat kriminal
2. Rumusan atau batasan tentang kejahatan dan penjahat dipaksakan sesuai dengan kepentingan mereka yang memiliki kekuasaan

---

[223] Schrag sebagaimana dikutip oleh Romli Atmasasmita, *op.cit*, hal. 39-40

3. Sesorang menjadi penjahat bukan karena ia melanggar undang-undang, malainkan karena ia ditetapkan demikian oleh penguasa
4. Sehubungan dengan kenyataan di mana setiap orang dapat berbuat baik dan tidak baik, tidak berarti bahwa mereka dapat dikelompokkan menjadi dua bagian: kelompok kriminal dan non kriminal
5. Tindakan penangkapan merupakan awal dari proses labeling.
6. Penangkapan dan pengambilan keputusan dalam sistemperadilan pidana adalah fungsi dari pelaku atau penjahat sebagai lawan dari karakteristik pelanggarnya
7. Usia, tingkatan sosial-ekonomi, dan ras merupakan karakteristik umum pelaku kejahatan yang menimbulkan perbedaan pengambilan keputusan dalam sistem peradilan pidana
8. Sistem peradilan pidana dibentuk berdasarkan perspektif kehendak bebas yang memperkenankan penilaian dan penolakan terhadap mereka yang dipandang sebagai penjahat
9. Labeling merupakan suatu proses yang akan melahirkan identifikasi dengan citra sebagai deviant dan sub kultur serta menghasilkan *rejection of the rejector*.

E.M. Lemert dapat juga dipandang sebagai arsitek teori labeling. Ia membedakan tiga bentuk penyimpangan dalam hubungannya dengan konteks kejahatan yang dilakukan, yaitu:

1. *Individual deviation*, timbulnya penyimpangan dari tekanan psikis dari dalam
2. *Situasional deviation*, yang merupakan hasil dari stres atau tekanan dan keadaan

3. *Systematic deviation*, adalah pola-pola dari perilaku kejahatan yang menjadi terorganisir dalam sub-sub kultur atau sistem tingkah laku.[224]

Lemert juga membedakan antara penyimpangan primer (*primary deviance*) dan penyimpangan sekunder (*secondary deviance*). *Primary deviance* ditujukan kepada perbuatan penyimpangan tingkah laku awal dari pelanggaran yang dianggap timbul karena berbagai hal dan oleh pelaku dipandang tidak berarti bagi kepribadiannya. *Secondary deviance* berkaitan dengan reorganisasi psikologis dari pengalaman seseorang sebagai akibat dari penangkapan dan cap sebagai penjahat. Sekali cap atau status itu dilekatkan pada seseorang, maka sangat sulit orang yang bersangkutan untuk selanjutnya melepaskan diri dari cap di maksud dan kemudian akan mengidentifikasikan dirinya dengan cap yang telah diberikan masyarakat terhadap dirinya.

Proses untuk menjadi secondary deviant tidak datang begitu saja, ada proses atau jalan untuk menuju jalan ke sana sebagaimana diungkapkan oleh Lemert:

> ... (1) primary deviation; (2) societal penalties; (3) further primary deviation; (4) stronger penalties and rejections; (5) further deviation, perhaps with hostilities and resentments beginning to focus upon those doing the penalizing; (6) crisis reached in the tolerance quotient, expressed in formal action by the community stigmatizing of the deviant; (7) strengthening of the deviant conduct as a reaction to the stigmatizing and penalties; (8) ultimate acceptance of deviant social status and efforts of adjusment on the basis of the associatied role.[225]

Meskipun teori labeling ini menawarkan pendekatan baru dalam mempelajari kejahatan, tidak berarti teori ini diterima begitu saja, artinya ada

---

224 I.S. Susanto, *op.cit*, hal. 77

225 Lemert sebagaimana dikutip oleh Frank P. Williams III and Marilyn D. McShane, *Criminological Theory*, Englewood Cliffs, New Jersey, Prentice Hall, 1988, hal. 89, sebagaimana dikutip oleh J.E. Sahetapy, *op.cit*, hal. 26-27

kritik yang mempersoalkan teori labeling ini. Kritik tersebut antara lain dikemukakan oleh **Gwynn Nettler**, antara lain:[226]

1. *Labeling theory does not explain the behaviours that lead to the application of labels.*

   Teori labeling menganggap tidak penting untuk mempersoalkan pentingnya faktor kausal dan nilai penjelasan yang bertalian dengan variabel personal. Teori ini lebih mengutamakan interpretasi politis daripada psikologis (sebagai suatu interpertasi yang didasarkan pada kriminologi positif). Teori ini memang menitikberatkan pada reaksi sosial masyarakat sehingga jika dipakai interpretasi psikologis akan mengalami kesulitan karena jumlah individu yang ada dalam masyarakat sangatlah banyak sehingga interpretasi psikologis akan memakan banyak waktu dan biaya sedangkan interpretasi politis lebih tepat karena reaksi yang ditimbulkan oleh masyarakat merupakan konstruksi sosial politis yang dilakukan oleh masyarakat setempat dan bukan konstruksi psikologis. Teori labeling menaruh perhatian pada rakyat lapisan bawah, golongan minoritas dan sejenisnya sehingga yang dipersoalkan adalah persoalan tentang kekuasaan yang diperoleh oleh mereka yang berkuasa yang menggunakan kekuasaanya itu untuk menekan kaum yang lemah. Pendirian ini membawa konsekuensi dan implikasi terhadap kebijakan publik dan politik kriminal.

2. *When applied to the understanding of individual behavior, the labeling hypothesis has low predictive power.*

---

[226] Gwynn Nettler sebagaimana dikutip oleh J.E. Sahetapy, *op.cit.*, hal. 27-28. Bandingkan dengan kritik serupa yang dikemukakan oleh Hagan dalam Romli Atmasasmita, *op.cit*, hal. 41.

Teori labeling mengingkari perbedaan dalam kepribadian, sesuatu yang dikatakan membohongi dirinya sendiri. Menurut teori ini *psychosis is not in her, but in her situation. "... when the mirrors in which she sees herself are changed, she will change".*

3. *The model of causation implicit in the labeling hypothesis is questionable.*

Teori ini meletakkan sebab musabab pada tempat yang tidak lazim, yaitu di tempat mereka yang bereaksi. Menurut **Sahetapy** para pakar teori ini seolah-olah tidak hendak berfikir atau tidak mau tahu tentang sebab dan akibat, yang ingin mereka pikirkan hanyalah semata-mata tentang interaksi saja. Apa yang dikemukakan **Gwynn Nettler** dan **Sahetapy** itu sepertinya berlebihan, karena teori labeling memang menitikberatkan pada reaksi masyarakat (berupa pemberian cap atau label pada pelaku kejahatan) artinya tidak membahas secara mendetail mengenai kepribadian si pelaku (yang telah menjadi titik berat kriminologi positif) dan tidaklah mungkin seorang penjahat mencap atau menerapkan label jahat pada dirinya sendiri, sesuatu yang dalam keadaan norma (kondisi sosial, ekonomi dan politis) sangat dihindari.

4. *On the level of social concerns, the labeling hypothesis does not answer the perennial questions about crime.*

Mengenai kritik ini **Sahetapy** mengatakan bahwa jika anda menanyakan mengapa sampai orang berbuat suatu kejahatan dan apa yang menyebabkan kejahatan makin bertambah atau makin berkurang, atau bagaimana dapat dilakukan upaya pencegahan kejahatan, maka hendaklah anda sadar bahwa anda tidak akan memperoleh suatu jawaban dari para pakar teori labeling ini.

Sekali lagi **Sahetapy** menilai keliru fokus dari teori labeling ini. Teori labeling tidak menjadikan pertanyaan mengapa seseorang melakukan kejahatan, mengapa kejahatan makin bertambah atau berkurang sebagai fokus utama, tetapi yang menjadi fokus utamanya adalah reaksi sosial masyarakat yang memberikan cap atau label penjahat kepada seseorang sehingga pertanyaan yang serupa dapat diajukan yaitu mengapa masyarakat memberikan cap atau label itu pada seseorang, adakah kepentingan tertentu di balik reaksi sosial masyarakat itu dan bagaimana perlakuan masyarakat terhadap penyandang cap atau label kriminal itu.

Kritik tidak selalu harus mematikan perkembangan suatu teori, kritik justru semakin mempertajam fokus studi kejahatan dengan adanya counter critic. Toeri labeling tidak sejelek seperti yang dikatakan **Gwynn Nettler** dan **Sahetapy** seperti di atas karena ada juga segi positif dari teori ini sebagaiman yang dikemukakan oleh **Frank P. Williams III** dan **Marilyn D. McShane** sebagai berikut:[227]

1. Society is characterized by multiple values with differing degrees of overlap
2. The quality of any individual behavior is determined only by the application of values. The identification of a behavior as deviant occurs through a reaction to that behavior.
3. Deviance is a quality of the reactionand is, not intrinsic to the behavior itself. If there is no reaction, there is no deviance
4. Once behavior is perceived by a social audience, and labeled deviant, the individual who engaged in that behavior is also labeled as a deviant.
5. The process of reacting and labeling is more likely when those being labeled are less socially powerful than their audience. Thus, deviance is more commonly ascribed to the less powerful in society

---

[227] Frank P. Williams III and Marilyn D. McShane, sebagaimana dikutip oleh J.E. Sahetapy, *op.cit*, hal. 28-29.

6. Reactors (individuals, social groups, law enforcement agencies) tend to observe more closely those whom they have identified as deviants and therefore they find even more deviance in these persons. Subsequent actsare reacted to more quickly and the label more firmly affixed.
7. The audience views an individual, once labeled, as being what the label says he or she is. A person labeled as a criminal perceived to be first and foremost a criminal; other attributes that are not covered by the label may be ignored.
8. In addition to "becoming" a deviant for the audience, an individual may begin to accept the label as a self-identity. Acceptance of the label depends upon the strength of the individual's original self-concept and the force of the labeling process.
9. A change in self-concept will result in an internalization of the deviant character, with all of its attributes
10. Further deviant behavior (secondary deviance) will be a product of living and acting within the role of the deviant label, often as a part of a deviant subculture.

3. Kriminalisasi, Dekriminalisasi dan Dépenalisasi

Pembicaraan mengenai kriminologi (dengan teori-teorinya yang telah berkembang) tidak akan berhenti selama masih ada kejahatan di masyarakat. Tetapi pembicaraan itu tidak bisa dilepaskan dari institusi lain, karena ada keterkaitan yang sangat erat antara kriminologi dengan institusi itu yaitu hukum terutama hukum pidana, bahkan sejak kelahirannya kriminologi dan hukum pidana mempunyai hubungan yang sangat erat.

Hukum memiliki keterikatan yang sangat luas dengan berbagai bidang ilmu, bahkan penguasaan ilmu hukum secara tunggal tidak akan dapat memecahkan masalah yang dihadapi masyarakat, sehingga diperlukan pengetahuan lain agar pemahaman terhadap permasalahan menjadi lebih jelas, tajam dan tidak simpang siur. Dengan berbekal pengetahuan hukum dan pengetahuan sosial lain, seperti sosiologi, psikologi, antropologi, religi, ekonomi, politik dan budaya maka diagnosa mengenai kesulitan-kesulitan yang

dihadapi masyarakat dapat lebih cermat, dan pemecahannyapun lebih dapat diterima oleh masyarakat.

Perkembangan kriminologi dari dahulu sampai sekarang tidak bisa dilepaskan dari keberadaan hukum pidana dan sosiologi hukum itu sendiri. Kriminologi, sosiologi dan dan hukum pidana memiliki lahan kajian yang satu sama lain saling berkaitan, sehingga tidak mengherankan apabila dengan memberdayakan ketiga kajian itu secara integral akan diperoleh pemahaman yang lebih baik dan mendekati kebutuhan senyatanya mengenai realitas kejahatan yang ada di masyarakat.

Kriminologi, khususnya sebagai pengaruh pemikiran kritis mengarahkan studinya pada proses-proses (kriminalisasi) baik proses pembuatan maupun bekerjanya undang-undang, dapat memberikan sumbangan besar di bidang sistem peradilan pidana khususnya berupa penelitian tentang penegakan hukum sehingga dapat digunakan untuk memperbaiki bekerjanya aparat penegak hukum.[228]

Permasalahan kriminalisasi, dekriminalisasi dan depenalisai adalah bidang kajian hukum pidana yang erat kaitannya dengan kriminologi. Ketiganya tidak bisa dilepaskan dari kriminologi apabila ingin mendapatkan pengetahuan yang luas dan keputusan yang komprehensif mengenai suatu masalah yang hendak dikriminalkan, didekriminalisasi atau didepenalisasi. Tanpa kajian kriminologi hukum pidana sebenarnya bisa melakukan ketiga hal tersebut, tetapi

---

[228] I.S. Susanto, *Kriminologi*, op.cit, hal. 14. Lihat juga Mulyana W. Kusumah, *Kriminologi* ..., op.cit, hal. 9

hasil yang dicapai tentunya tidak akan selengkap dan sebaik apabila menggunakan bantuan kriminologi.

Kriminalisasi merupakan suatu proses penetapan suatu perbuatan yang semula bukan tindak pidana menjadi tindak pidana. Untuk menetapkan suatu perbuatan yang sebelumnya tidak dikategorikan sebagai tindak pidana menjadi perbuatan yang dikategorikan sebagai tindak pidana bukanlah suatu pekerjaan yang mudah. Proses kriminalisasi berakhir dengan terbentuknya undang-undang yang menetapkan perbuatan yang itu dilarang dan diancam dengan sanksi yang berupa pidana.[229]

Tidak mudah untuk menetapkan suatu perbuatan sebagai suatu tindak pidana, artinya ada beberapa proses yang harus dilalui. Selain kajian yang mendalam mengenai perbuatan itu dari sudut kriminologi, maka harus dipertimbangkan pula beberapa hal yang perlu diperhatikan, yaitu tujuan hukum pidana itu sendiri, penetapan perbuatan yang tidak dikehendaki, perbandingan antara sarana dan hasil dan kemampuan badan penegak hukum.[230]

Hukum pidana mempunyai sifat *ultimum remidium* atau alat terakhir yang berisi pengenaan penderitaan kepada pelaku kejahatan. Sifat hukum pidana ini menyebabkan hukum pidana dinilai sangat kejam sehingga pengenaannya haruslah merupakan upaya terakhir apabila upaya-upaya lain tidak dapat dilakukan untuk memperbaiki pelaku kejahatan. Mengingat sifat kejamnya hukum pidana ini, maka penetapan suatu perbuatan dengan ancaman hukumannya haruslah memperhatikan berbagai aspek kemanusiaan. Proses

---

229 Sudarto. *Hukum dan Hukum Pidana*, Alumni, Bandung, 1986, hal. 32 dan 151
230 *Ibid*, hal, 36

kriminalisasi dalam hal ini tidak boleh dilakukan sembarangan karena hal ini menyangkut harkat, martabat dan hak asasi manusia untuk hidup.

Penetapan suatu perbuatan menjadi tindak pidana atau bukan haruslah didasarkan pada pertimbangan yang matang. Penetapan ini harus dijauhkan dari unsur-unsur politis sehingga mereka yang mempunyai kekuasaan tidak dapat mempengaruhi pembuat undang-undang agar perbuatan jahatnya tidak terkena jerat hukum. Meskipun ada anggapan bahwa undang-undang adalah hasil dari kompromi politis, tetapi sebisa mungkin unsur politis yang merugikan berbagai pihak (terutama mereka yang tidak punyai kekuasaan untuk mempengaruhi pembuat undang-undang) dapat ditekan atau diminimalisir.

Penetapan suatu perbuatan menjadi tindak pidana harus pula memperhatikan perbandingan antara sarana dan hasil serta kemampuan aparat penegak hukum. Apabila sarana yang diperlukan dan kemampuan aparatnya tidak memadai maka penetapan suatu perbuatan menjadi tindak pidana menjadi tidak berarti karena sarana untuk menegakkannya tidak ada sehingga penetapan itu hanya menjadi macan kertas saja, tidak ada implementasinya dan hanya merupakan pemborosan anggaran negara.

Dari uraian tersebut maka dapatlah dikatakan bahwa proses kriminalisasi merupakan proses yang tidak hanya bersifat sosial tetapi juga politis. Pandangan hidup yang ada dan dipelihara oleh masyarakat atau pemegang kekuasaan akan mewarnai hasil kriminalisasi. Menarik sekali apa yang dikatakan oleh **Richard Quinney** mengenai kriminalisasi ini. Ia mengatakan *"criminal laws are formulated within a social context that involves the promotion of the interests of certain groups in society."*

Dalam kaitannya dengan kriminalisasi ini, menarik sekali apa yang dikemukakan oleh **Hulsman** dalam suatu pertemuan di Bellagio (Italia) tahun 1973 yang diselenggarakan oleh Centro Nasionale di Prevenzione e Diffesa Sociale, di mana disebutkan beberapa kriteria absolut yang perlu diperhatikan:[231]

a. Criminalization must never be founded solely on the desire to impose a specific moral attitude to a given type of behaviour.
b. The main reason for making an act a criminal offence should never be to establish a framework for helping or treating a potential offender in his own interest.
c. Criminalization must not result in overloading the capacity of penal machinery
d. Criminalization should never serve as a screen to what is only an apparent solution to a problem.

Dekriminalisasi adalah suatu proses penghapusan sama sekali sifat dapat dipidananya suatu perbuatan yang semula merupakan tindak pidana dan juga penghapusan sanksinya berupa pidana. Dalam proses dekriminalisasi ini tidak hanya kualifikasi pidana saja yang dihapuskan tetapi juga sifat melawan hukum atau melanggar hukumnya, lebih dari itu adalah penghapusan sanksi negatif itu tidak diganti dengan reaksi sosial lain baik perdata maupun administrasi.[232]

Dalam proses dekriminalisasi ini penelitian kriminologi diperlukan untuk menentukan apakah perbuatan itu layak didekriminalisasikan dan

---

231 Hulsman sebagaimana dikutip oleh Sudarto, *ibid*, hal. 41
232 *Ibid*, hal. 32

bagaimana kemungkinannya di masa yang akan datang. Tidak menutup kemungkinan perbuatan yang telah didekriminalisasikan di masa mendatang oleh masyarakat dituntut untuk dikriminalisasikan sehingga kajian mengenai manfaat dan kerugian dekriminalisasi haruslah mendapat perhatian.

Suatu proses dekriminasliasi dapat terjadi karena beberapa sebab, seperti misalnya (contoh init tidak bersifat limitatif):[233]

a. Suatu sanksi secara sosiologis merupakan persetujuan (sanksi positif) atau penolakan terhadap pola perilaku tertentu (sanksi negatif). Ada kemungkinan bahwa nilai-nilai masyarakat mengenai sanksi negatif tertentu terhadap perilaku tertentu mengalami perubahan, sehingga perilaku yang terkena sanksi-sanksi tersebut tidak lagi ditolak.
b. Timbulnya keragu-raguan yang sangat kuat akan tujuan yang ingin dicapai dengan penetapan sanksi-sanksi negatif tertentu
c. Adanya keyakinan yang kuat, bahwa biaya sosial untuk menerapkan sanksi-sanksi negatif tertentu sangat besar.
d. Sangat terbatasnya efektivitas dari sanksi-sanksi negatif tertentu sehingga penerapannya akan menimbulkan kepudaran kewibawaan hukum.

Dalam kaitannya dengan kriminalisasi dan dekriminalisasi ini, Simposium Pembaharuan Hukum Pidana Nasional pada bulan Agustus 1980 dalam salah satu laporannya menyatakan[234]

> Masalah kriminalisasi dan dekriminalisasi atas suatu perbuatan haruslah sesuai dengan politik kriminil yang dianut oleh bangsa Indonesia, yaitu sejauh mana perbuatan tersebut bertentangan atau

---

[233] Soerjono Soekanto dkk, *op.cit*, hal. 47-48

[234] Laporan Simposium Pembaharuan Hukum Pidana Nasional 1980 di Semarang, seperti dikutip oleh Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Hukum Pidana*, BP UNDIP Semarang, 1994, hal. 36

> tidak bertentangan dengan nilai-nilai fundamental yang berlaku dalam masyarakat dan oleh masyarakat dianggap patut atau tidak patut dihukum dalam rangka menyelenggarakan kesejahteraan masyarakat.

Khusus mengenai kriteria kriminalisasi dan dekriminalisasi, laporan simposium itu menyatakan

> Untuk menetapkan suatu perbuatan itu sebagai tindakan kriminil, perlu memperhatikan kriteria umum sebagai berikut:
> 1. Apakah perbuatan itu tidak disukai atau dibenci oleh masyarakat karena merugikan atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban;
> 2. Apakah biaya mengkriminalisasi seimbang dengan hasilnya yang akan dicapai, artinya cost pembuatan undang-undang, pengawasan dan penegakan hukum, serta beban yang dipikul korban, pelaku dan pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai;
> 3. Apakah akan makin menambah beban aparat penegak hukum yang tidak seimbang atau nyata-nyata tidak dapat diemban oleh kemampuan yang dimilikinya
> 4. Apakah perbuatan-perbuatan itu menghambat atau menghalangi cita-cita bangsa Indonesia, sehingga merupakan bahaya bagi keseluruhan masyarakat.[235]

Depenalisasi merupakan proses penghapusan ancaman pidana (sehingga ancaman pidananya itu hilang) terhadap perbuatan yang semula merupakan tindak pidana, akan tetapi masih dimungkinkan adanya penuntutan secara lain.[236] Hal ini dapat dilakukan mengingat sifat hukum pidana sebagai *ultimim remidium*, di mana ancaman pidana yang ada dianggap tidak aspiratif atau terlalu berat, sehingga perlu diganti dengan ancaman pidana lain yang lebih ringan dan manusiawi.

---

[235] Bandingkan dengan kriteria yang dikemukakan oleh Bassiouni dalam Barda Nawawi Arief, *ibid*, hal. 36-37

[236] Sudarto, *op.cit*, hal. 151

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. KONSTRUKSI HACKING SEBAGAI KEJAHATAN

1. Pengertian dan Pembedaan Hacker, Craker dan Bogus Hacker

Sampai saat ini sering terdapat kekeliruan dalam menuliskan istilah yang tepat untuk mereka yang melakukan perusakan terhadap situs milik publik atau pribadi. Istilah yang sering digunakan oleh media cetak dan elektronik adalah *hacker*, padahal yang tepat adalah *cracker*.[1] Kesalahan penggunaan istilah ini menyebabkan apa yang dipahami oleh masyarakat mengenai gambaran tingkah laku hacker adalah negatif. Untuk itulah pemahaman mengenai perbedaan antara hacker dan cracker diperlukan dalam pembahasan ini agar tidak terjadi atau tercipta pengertian yang salah mengenai makna hacker dan cracker.

Untuk memahami pembedaan dan penggunaan kedua istilah tersebut maka dipandang perlu untuk melihatnya dari sisi sejarah perkembangan dan penggunaan istilah tersebut. Sejarah hacker sendiri tidak bisa dilepaskan dari

---

[1] Hal ini terlihat dari penggunaan istilah hacker yang sebenarnya lebih tepat digunakan oleh berbagai media massa, seperti di harian Republika, 26 September 1999, 16 Januari 2000, 17 Februari 2000, 22 Agustus 2000; Reuter, February 15, 2000, Media Indonesia, 2 September 2000, Associated Press, February 15, 2000, Suara Pembaruan, 22 Juli 2000. Kesalahan dalam menggunakan istilah ini (berupa penyamaan makna hacker dan cracker) juga terjadi pada beberapa buku yang antara lain ditulis Neil Barrett, Digital Crime, Policing the Cybernation Kogan Page Ltd, London, 1997, Mark D. Rasch, *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, Computer Law Association; 1996, versi elektronik dapat dijumpai di http://cla.org/RuhBook/chp11.htm dan masih banyak lagi.

sejarah perkembangan komputer dan jaringan komputer. Secara umum sejarah hacker dapat dibagi dalam tiga gelombang, yaitu[2]

a. Hacker gelombang pertama

Hacker gelombang pertama atau awal perkembangan hacker terpusat di sekitar Massachusetts Institute of Technology (MIT) pada tahun 1950-an dan 1960-an. Para pemula atau perintis hacker ini adalah mahasiswa MIT yang memiliki rasa ingin tahu dan kepandaian untuk mengeksplorasi peralihan jaringan telepon (*the phone switching networks*) dan sistem kontrol pada Tech Model Railroad Club dan menyusun komputer di MIT Artificial Intelegence Laboratorium (MIT AI Lab). Direktur laboratorium itu, **Marvin Minsky**, menaruh simpati dan cukup berkesan dengan keinginan dan kepandaian para hacker untuk mengeksplorasi hal tersebut di atas. Dia juga mengijinkan para hacker itu secara langsung menghubungkan (*access*) dengan mesin. Di antara para hacker itu telah keluar dari sekolah (*dropped out*) dan menghabiskan waktunya untuk melakukan kegiatan hacking. Termasuk figure hacker legendaris pada gelombang pertama ini adalah **Peter Deutsch, Bill Grosper, Richard Greenblatt, Tom Knight** dan **Jerry Sussman.**

Waktu itu adalah usia emas para hacker komputer, meskipun pada saat itu para hacker dihadapkan pada persoalan keadaan mesin yaitu mesin yang besar, lambat, tidak praktis untuk dipergunakan dan kelihatannya memerlukan usaha yang keras untuk membuat komputer itu dapat bekerja secara sederhana untuk menghitung. Meskipun kejadian tersebut telah

---

[2] Disarikan dari Erick Brunvand, *The Heroic Hacker: Legends of the Computer Age*, last update 15 Oktober 1996, versi elektronik dapat dijumpai di http://www.cs.utah.edu/~elb/node3.html.

berlangsung lebih dari 40 tahun yang lalu, para programer saat ini menyukai usaha mereka dan melihatnya melalui cerita mengenai asal mula penghitungan dengan mesin. Prestasi perintis hacker yang legendaris itu membuat semuanya lebih menakjubkan karena peralatan atau mesin yang digunakan terlihat primitif dan lebih layak untuk dibuang.

b. Hacker gelombang kedua

Komputer dengan cepat menyebar ke negara bagian lain di Amerika Serikat, demikian juga dengan budaya hacker. Sebagian besar penyebarannya adalah inisiatif dari hacker yang telah mulai di MIT. Pada pertengahan 1960-an, terlihat pusat pengembangan budaya hacker ada di universitas lain seperti Carnegie Mellon University dan Stanford University. The Stanford AI Lab (SAIL) di bawah direksi **John McCarthy**, menjadi pusat untuk aktivitas hacker di pesisir barat Amerika Serikat. Ketika mesin SAIL akhirnya mati (*shut down*) pada 1991, para hacker mengirim e-mail yang berisi pesan selamat tinggal kepada Internet sebagaimana mesin SAIL itu mengirimkan ucapan terakhir kepada teman.

Pada waktu itu setiap pusat penelitian (untuk kepentingan) komersial menjadi rumah bagi hacker. Perusahaan-perusahaan seperti ATT, Xerox dan lainnya semuanya mempunyai programer yang mempunyai keahlian untuk menjadi hacker. Termasuk dalam hacker legendaris gelombang kedua dan aktif berakitivitas antara lain **Ed Fredkin, Brian Reid, Jim Gosling, Brian Kernighan, Dennis Ritchie** dan **Richard Stallman.**

c. Hacker gelombang ketiga

Gelombang ketiga dari aktivitas hacker lahir di California sebelah utara tanpa ada hubungan langsung (silsilah) dengan hackers MIT. Hacker ini

dimulai dengan Himebrew Computer Club di San Fransisco. Klub ini adalah kelompok pecinta elektronik dengan kebiasaan menarik dan mempunyai ide radikal untuk membangun komputer mereka. Karena persoalan ukuran dan harga dari komputer terbaru, maka setiap hacker membatasi penggunaan angka kecil (*small number*) dari mesin yang dibangun oleh perusahaan besar dan menginstal di universitas atau pusat penelitian industri. Hacker gelombang ketiga ini menginginkan mesin mereka tidak hanya dapat diprogram di rumah tetapi juga dapat dibangun dan dimodifikasi dengan hardware komputer dari rumah. Mereka yang termasuk kelompok hacker gelombang ketiga dan termasuk figur legendaris adalah **Lee Felsenstein, Steve Dompier, Steve Wozniak, Steve Jobs** dan **Bill Gates.**

Hacker gelombang pertama adalah sekelompok orang yang pertama kali menggunakan istilah *hack* untuk teknik-teknik yang dipakai pada pemrograman kreatif yang mempu memecahkan masalah secara lebih efisien daripada teknik biasa. Hacker-hacker inilah yang membantu pengembangan bahasa LISP (bahasa pada sistem atau program komputer) yang diciptakan oleh **John McCarthy,** Direksi The Stanford AI Laboratorium.[3]

Hacker gelombang kedua telah berhasil membuat sistem operasi sendiri untuk minikomputer mereka (penyempurnaan dari PDP-10) dan membuat berbagai program bantunya sendiri yang kebanyakan masih dalam bahasa LISP. Perkembangan yang menarik pada gelombang ini adalah kelahiran sistem operasi UNIX karya **Ken Thompson** dan **Dennis Ritchie** (Bell Labs). Sistem operasi inilah yang kemudian dalam perkembangannya digunakan secara umum

---

[3] *Ibid.*.

untuk membangun jaringan komputer baik *local* maupun *wide area network*. **Dennis Ritchie** juga menciptakan bahasa C (yang merupakan pengembangan bahasa pemrograman B yang diciptakan oleh **Ken Thompson**) yang digunakan untuk sistem operasi UNIX yang amat populer dan mempermudah para programer dan hacker.[4]

Setelah komputer yang berukuran raksasa telah digantikan oleh komputer pribadi yang berukuran lebih kecil dan telah menyebar ke rumah-rumah sebagai akibat penemuan komputer pribadi itu oleh **Steve Jobs** dan **Steve Wozniack** maka jumlah hacker semakin meningkat dengan sendirinya. Hacker pada masa ini (gelombang ketiga) berbeda dengan hacker pada masa sebelumnya (di MIT) karena hacker masa ini lebih sering berkutat dengan perangkat lunak. Sebagian dari hacker gelombang ketiga ini menjadi sukses menjadi usahawan di bidang komputer, seperti **Bill Gates** dengan Microsoftnya, **Steve Wozniak** dan **Steve Jobs** melalui Apple Computernya.[5]

Sebenarnya sejarah perkembangan hacker tidak terbatas pada ketiga gelombang tersebut, karena pada tahun 1990-an muncul gelombang baru perkembangan hacker. Tetapi pada tahun 1990-an ini istilah hacker semakin buruk karena dikonotasikan sebagai orang-orang jahat yang melakukan perusakan terhadap situs milik publik atau pribadi. Jumlah mereka atau cracker dari tahun ke tahun mengalami penambahan yang oleh hacker sejati tak bisa dibendung. Mereka tergabung dalam berbagai kelompok-kelompok cracket, seperti yang tergabung dalam kelompok *hacker underground*. Mereka yang masuk dalam gelombang ini (tanpa membedakan hacker dan cracker) antara lain

---

4 *Ibid.*
5 *Ibid.*

Robert Tappan Morris, Kevin Poulsen, Linus Benedict Torvalds, Kevin Mitnick, Tsutomu Shimomura dan masih banyak lagi.[6]

Sejak munculnya komputer pribadi, maka muncul jaringan komputer baru yang dinamakan UNIX to UNIX CoPy (UUCP) pada tahun 1976 dan USENET pada tahun 1979. Kemudian pada akhir tahun 1970-an muncul sebuah konsep jaringan baru yaitu *Bulletin Board System* (BBS) yang dimulai oleh **Ward Christiansen** dan **Randy Sues** dan pada tahun 1982 ditetapkan protokol TCP/IP sebagai protokol ARPANET. Perkembangan-perkembangan tersebut semakin mempercepat informasi yang disalurkan dan meningkatkan jumlah hacker secara signifikan.

Dalam sejarah hacker, apa yang dilakukan oleh para hacker itu selalu ada kaitannya dengan pengembangan sistem keamanan komputer. Keamanan komputer itu penting untuk melindungi data-data atau informasi yang bersifat rahasia dan agar tetap terjaga kerahasiaannya maka sistem keamanan yang ada dan digunakan untuk melindunginya perlu secara terus menerus dimodifikasi atau selalu dijaga kemutakhirannya. Tugas hacker adalah menguji sistem keamanan ini dan memperbaikinya sistem atau program keamanannya sehingga tidaklah mengherankan jika seorang hacker adalah seorang programer (tetapi tidak setiap programer bisa menjadi hacker).[7]

---

[6] *Ibid.*.

[7] Selain berkaitan dengan pengembangan sistem keamanan komputer atau jaringan komputer, seorang hacker yang melakukan hacking juga sangat bermanfaat dalam meningkatkan kecepatan program dan menghemat sumber daya yang ada. Kelemahan yang dimiliki oleh sebuah program akan diketahui oleh seorang hacker dan ia akan memberitahukan kepada pemilik atau pembuat program untuk segera memperbaiki atau menyempurnakan. Dari kelemahan sebuah program yang telah diketahui, tidak hanya program itu yang dapat disempurnakan, tetapi kecepatan yang dimiliki sebuah komputer (lengkap dengan sistem operasinya) akan bertambah, seperti sistem operasi Windows 3.1 lebih lambat jika dibandingkan dengan Windows 95 dan seterusnya.

Seiring dengan perkembangan komputer dan jaringan komputer, maka pengertian hacker juga terus mengalami perubahan dan perkembangan. Jika pada tahun 1994, **Eric S. Raymond** mengartikan hacker dalam lima kategori, maka dalam perkembangannya, hacker memiliki delapan arti, yaitu:[8]

a. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
b. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming
c. A person capable of appreciating hack value
d. A person who is good at programming quickly
e. An expert at a particular program, or one who frequently does work using it or on it; as in "a UNIX *Hacker*" (Definition a through f are correlated, and people who fit them congregate)
f. An expert or enthusiast of any kind. One might be an astronomy hacker for example
g. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
h. (Deprecated) A malicious meddler who tries to discover sensitive information by poking around. Hence password hacker, "network hacker". The correct term for this sense is "*cracker*"

Dari definisi tersebut dapatlah disimpulkan bahwa hacker bukanlah orang yang suka merusak situs milik publik atau pribadi dengan tujuan untuk kesenangan atau kejahatan, tetapi hacker yang juga seorang programer selalu melakukan aktivitasnya untuk memperbaiki dan meningkatkan kemampuan program yang dibuat (atau dibuat orang lain). Dalam bahasa yang lain, **Bruce Sterling** mengatakan "*Hackers are very serious about forbidden knowledge. They are possessed not merely by curiosity, but by a positive lust to know.*"[9]

Hacker pada dasarnya adalah orang yang bergelut dengan sistem pemrograman secara terperinci dan berusaha untuk terus mendongkrak

---

8 *Who is this Guy who Calls Himself Hacker One*, versi elektronik dapat dijumpai di http://www.im.lcs.mit.edu/gilliam/hacker-one.html.

9 Bruce Sterling, *The Hacker Crackdown, Law and Disorder on the Electronic Frontier*, Market Paperback, 1994, versi elektronik dapat dijumpai di http://www.lysator.Liu.se/etexts/hacker/

kemampuannya. Seorang hacker juga bukan sekedar orang yang berteori tentang pemrograman atau berdiskusi tentang hal itu, tetapi ia juga seorang praktisi. Tetapi di sini perlu dicatat bahwa seorang programer belum tentu seorang hacker karena seorang hacker adalah orang yang mampu mengapresiasi nilai-nilai tertentu dalam urusan hacking. Ia harus seorang yang memahami seluk beluk pemrograman secara cepat dan menggunakannya secara tepat.

Sikap seorang hacker sama seperti sikap orang yang baik pada umumnya, sama seperti sikap seorang ilmuwan pada umumnya yang selalu ingin mencari tahu dan meneliti segala sesuatu untuk mendapatkan kebenaran atau menemukan sesuatu yang dapat bermanfaat bagi umat manusia maupun bagi perkembangan ilmu pengetahuan dan teknologi itu sendiri. Hacker senang belajar pemrograman dan melakukan praktek atau latihan pemrograman itu serta menyebarluaskan ilmunya tersebut.

Secara ideal hacker membuat informasi menjadi tersebar lebih luas dan membuat arus teknologi menjadi lebih baik bagi banyak orang. Dengan statusnya itu seorang hacker seringkali berjuang dengan informasi-informasi palsu atau bertualang dalam penjelajahan digital yang sangat menantang. Hacker juga bukan seorang yang menulis virus komputer yang mematikan seperti virus *I love you* dari **Onel de Guzman**, yang menciptakan virus adalah seorang progamer dan kebetulan **Onel de Guzman** adalah seorang programer. Tetapi hal tersebut tidak serta merta dapat menyebut seorang programer adalah orang yang jahat atau kriminal bahkan pada umumnya seorang programer justru membantu suatu sistem komputer agar bisa bekerja untuk kebutuhan-kebutuhan tertentu.

Hacker selalu berusaha untuk menyelesaikan masalah dan membuat sesuatu berguna meskipun dalam jumlah yang tidak terlalu besar. Hacker percaya pada kebebasan dan kerjasama secara sukarela. Sikap hacker ini harus diyakini oleh mereka yang berminat menjadi hacker dan berbuat seolah-olah memiliki sikap ini. Tetapi jika mereka yang berminat menjadi hacker (atau dapat diterima di lingkungan hacker) dan berniat untuk menumbuhkan sikap hacker tanpa meyakininya, maka mereka belum menangkap maknanya. Menjadi orang yang meyakini sikap hacker penting bagi mereka yang berminat menjadi hacker agar bisa terus belajar dan termotivasi.

Hacker adalah orang yang kreatif, dan seperti orang kreatif lainnya, ia selalu berusaha untuk selalu membuat hal yang baru (dari yang tidak ada menjadi ada) atau memodifikasi atau memperbaiki sesuatu (barang) yang lama sehingga tampak baru dan lebih bermanfaat. Tetapi seni kreatif yang paling mudah dan efektif (cepat diperoleh dan murah biayanya) adalah dengan cara meniru (dalam hal ini Jepang dapatlah dijadikan sebagai pelajaran bagaimana dia dengan cara meniru dapat menikmati kemajuan seperti sekarang). Untuk menjadi seorang hacker dapat juga dilakukan dengan cara meniru dari para ahlinya. Bukan hanya meniru para ahli tersebut secara intelektual saja tetapi juga secara emosional.

Untuk menjadi hacker, selain harus belajar bahasa pemrograman atau meniru (cara yang paling mudah) maka pernyataan-pernyataan berikut ini dapat diikuti dan diyakini. Jika mereka yang berminat menjadi hacker mengikuti dan

meyakini pernyataan-pernyataan ini ada kemungkinan dapat diterima di lingkungan hacker. Pernyataan-pernyataan tersebut adalah:[10]

a. Dunia penuh dengan persoalan-persoalan menarik yang menanti untuk dipecahkan (*The world is full of fascinating problems waiting to be solved*)

   Bagi hacker hidup adalah tantangan dan tantangan itu harus selalu dihadapi dan dipecahkan. Menjadi hacker sebetulnya menyenangkan, tetapi menyenangkan yang menuntut usaha. Setiap kesenangan membutuhkan usaha dan setiap usaha membutuhkan motivasi, seperti halnya seorang atlet selalu termotivasi untuk selalu menjadi juara. Untuk menjadi seorang hacker, maka mereka yang berminat harus termotivasi untuk memecahkan persoalan, mengasah keahlian dan melatih kecerdasan. Mereka yang tidak tertarik untuk memecahkan suatu persoalan (khususnya persoalan mengenai komputer atau jaringan komputer), tidak mencoba keahlian dan melatih kecerdasan dalam hal pemrograman dan hacking, jangan harap bisa menjadi hacker.

b. Tidak seharusnya masalah yang sama dipecahkan dua kali (*Nobody should ever have to solve a problem twice*)

   Otak yang kreatif merupakan sumber daya yang berharga dan terbatas dan tidak seharusnya sumber daya ini diboroskan karena ada begitu banyak masalah menarik baru lain di dunia ini yang menanti. Untuk dapat bertingkah laku seperti hacker, mereka yang berminat harus percaya bahwa waktu berfikir hacker lain itu berharga, sebegitu berharganya hingga merupakan suatu kewajiban moral bagi mereka untuk membagikan

---

[10] Disarikan dari tulisan Eric S. Raymond, *How To Become A Hacker*, edisi revisi 1.92, September 2000, versi elektronik dapat dijumpai di http://www.tuxedo.org/~esr/faqs/hacker-howto.html

informasi, menyelesaikan masalah lalu memberi jawabannya pada hacker lain supaya mereka menyelesaikan masalah baru dan tidak selamanya berkutat pada masalah-masalah lama.

Seorang hacker tidak harus berkeyakinan bahwa semua produk kreatifnya harus direlakan bagi orang lain meski hacker yang demikianlah yang paling dihormati hacker lain. Menurut nilai-nilai hacker, jual atau memberi informasi sebagian, asal cukup untuk hidup dan tetap dapat memakai komputer sudahlah cukup. Tidaklah melanggar nilai hacker jika memanfaatkan ilmu yang dimilikinya untuk membiayai keluarga atau bahkan menjadikan diri kaya, asalkan anda tetap mengingat diri sebagai seorang hacker.

c. Kebosanan dan pekerjaan membosankan itu jahat (*Boredom and drudgery are evil*)

Hacker (dan manusia kreatif pada umumnya) tidak seharusnya dibosankan dengan pekerjaan yang berulang-ulang, karena pekerjaan yang demikian kadang-kadang sangat membantu dalam meningkatkan kemampuan teknis dan analitisnya. Perilaku ini tidak berarti hacker tidak menyukai pekerjaan baru, justru pekerjaan baru itulah yang menjadikan hacker tertantang untuk menyelesaikan persoalan-persoalan baru. Kebosanan yang dimiliki hacker merupakan pemborosan sumber daya dan karena itu kebosanan dan pekerjaan membosankan bukan saja tidak menyenangkan tetapi juga jahat.

Untuk bertingkah laku seperti hacker, mereka harus meyakini hal ini sehingga mereka itu mempunyai keinginan untuk mengotomasi sebanyak

mungkin bagian yang membosankan, bukan saja bagi diri sendiri tetapi juga bagi orang lain (terutama sesama hacker)

d. Kebebasan itu baik (*Freedom is good*)

Kebebasan itu hak asasi dan milik semua manusia, termasuk hacker yang membutuhkannya, terutama untuk mewujudkan seni kreatifnya. Pembatasan atau larangan terhadap daya kreatifnya merupakan hambatan yang dapat menahan laju pengembangan ilmu pengetahuan dan tehnik hacking yang dimilikinya. Secara alamiah hacker anti otoriter dan siapapun yang dapat memerintah hacker akan dapat menghentikan hacker itu untuk menyelesaikan persoalan yang menarik. Jadi sikap otoriter bagi para hacker harus dilawan di manapun para hacker itu berada, agar nantinya tidak menekan atau membatasi kemajuan yang hendak dicapai oleh hacker.

Salah satu sikap para penguasa otoriter adalah selalu hidup di atas sensor dan kerahasiaan, mereka tidak percaya pada kerjasama dan berbagi informasi dan satu-satunya jenis kerjasama yang disukai adalah yang dapat mereka kendalikan. Jadi untuk bertindak seperti seorang hacker, mereka perlu mengembangkan rasa benci pada penyensoran, kerahasiaan dan penggunaan kekerasan atau penipuan untuk memaksakan kehendak pada orang lain. Selain itu mereka juga harus bersedia bertindak demi keyakinan itu.

e. Sikap saja tak ada artinya tanpa kemampuan (*Attitude is no substitute for competence*)

Apa yang diuraikan di atas dapat diikuti sebagai suatu sikap tindak para hacker. Sikap ini dalam perkembangannya kemungkinan berubah atau disesuaikan karena jumlah hacker tiap tahun selalu bertambah dan mereka

tentunya memiliki latar belakang pendidikan, politik, sosial, ekonomi dan budaya sendiri. Tetapi bagi seorang hacker, memiliki sikap dan mengembangkannya belum membuat seseorang menjadi hacker. Selain sikap, untuk menjadi seorang hacker dibutuhkan kecerdasan, latihan, dedikasi dan kerja keras.

Jadi mereka yang ingin menjadi hacker perlu belajar untuk tidak mempercayai sikap dan menghormati setiap bentuk kemampuan. Hacker tidak bersedia menghabiskan waktu dengan orang-orang yang hanya bersikap seperti hacker (padahal bukan hacker), tetapi mereka memuja kemampuan, terutama kemampuan dalam hacking. Bagi hacker kemampuan di bidang apapun adalah baik dan yang utama baginya adalah kemampuan untuk mengatasi hidup yang sulit yang hanya dapat dikuasai oleh sedikit orang. Bagi hacker yang terbaik adalah kemampuan dalam bidang yang sulit dan melibatkan ketajaman mental, keahlian serta konsentrasi.

Dunia hacker berjalan di atas reputasi dan reputasi tersebut di atas hanya dapat dinilai oleh rekan sejawat. Reputasi itu dinilai dari kemampuan yang dimilikinya dan cara yang dilakukan serta hasil yang diperoleh dalam menyelesaikan suatu persoalan. Jika reputasi dan kemampuan yang dimiliki ini benar-benar dijalankan secara konsisten maka hacker lain akan menilainya sebagai seorang hacker. Tegasnya dunia hacker merupakan dunia yang oleh para antropolog disebut sebagai budaya memberi. Kedudukan dan reputasi tidak diperoleh dengan menguasai orang lain atau dengan memiliki sesuatu yang tidak dimiliki orang lain, tetapi dengan memberikan sesuatu. [11]

---

[11] *Ibid*

Sikap hacker yang positif itu dalam perkembangannya mengalami pembiasan atau citranya menjadi buruk karena terjadi penyalahgunaan kemampuan untuk memperoleh kesenangan, kekayaan melalui cara-cara yang oleh lingkungan hacker sendiri sebenarnya tidak disukai. Pembiasaan arti ini terjadi karena informasi mengenai teknik-teknik hacking menyebar secara luas dan dimanfaatkan oleh orang lain untuk melakukan kejahatan. Mereka inilah yang disebut dengan ***Cracker*** atau hacker topi hitam. Cracker ini dapat mempunyai kemampuan seperti hacker (berupa kemampuan pemrograman dan sebagainya) dan dapat pula tidak. Cracker yang tidak mempunyai kemampuan seperti hacker adalah mereka yang memanfaatkan informasi dari hacker (sebagai wujud budaya memberi kepada siapa saja) dan memanfaatkan informasi itu untuk melakukan kegiatan hacking atau disesuaikan dengan istilah pelakunya dinamakan *cracking*. Cracker yang tidak mempunyai kemampuan seperti hacker ini sering disebut dengan istilah ***Bogus Hacker*** atau ***vandal komputer.***

Jadi yang membedakan antara hacker dengan cracker yang utama adalah dalam hal *niat*. Hacker (atau disebut juga hacker topi putih) mempunyai niat yang luhur, sedangkan cracker mempunyai niat jahat berupa keinginan untuk merusak atau menguasai atau ingin memiliki sesuatu. Perbedaan kedua adalah dalam masalah *kemampuan*, cracker tidak harus atau tidak selalu memiliki kemampuan seperti yang dimiliki oleh hacker (seperti pemrograman), tetapi seorang hacker sejati adalah seorang programer. Perbedaan ketiga dalah dalam hal *sifat*. Hacker selalu memegang teguh sifat atau prinsip-prinsip seorang hacker (seperti telah disebutkan di atas), tetapi cracker tidak memiliki (atau memiliki tetapi tidak mematuhi) sifat seperti hacker. Perbedaan keempat

adalah dalam masalah *etika*. Hacker selalu memegang teguh dan mematuhi etika hacker dalam melakukan aktivitasnya, sedangkan cracker dalam melakukan aksinya sama sekali tidak mematuhi etika tersebut. Bagi cracker, etika bukanlah prinsip atau pedoman tingkah laku yang harus dituruti atau diikuti, tetapi rasa senang dan kebanggaan bisa membobol atau merusak situs milik orang atau badan hukum lain yang harus dijadikan pedoman aktivitasnya.

Dalam *The New Hacker's Dictionary* disebutkan bahwa yang dimaksud dengan cracker adalah

> One who breaks security on a system. Coined by hackers in defense against journalistic mususe of the term "hacker." The term "cracker" reflects a strong revulsion at the theft and vandalism perpetrated by cracking rings. There is far less overlap between hackerdom and crackerdom than most would suspect.[12]

Shailen S. Mistry dalam situsnya mengartikan cracker sebagai *these are the hackers that break into systems. Though not all hackers crack, all crackers are hackers by definition.*[13]

Hacker sejati tidak suka bergaul dengan cracker dan memandang cracker sebagai orang malas, tidak bertanggung jawab dan tidak cerdas. Hacker sejati tidak setuju jika dikatakan bahwa dengan menerobos sistem keamanan, seseorang telah menjadi hacker. Perbedaan lain yang mencolok (selain yang telah disebutkan di atas) adalah hacker sifatnya membangun sedangkan cracker sifatnya membongkar.

Salah satu yang membedakan antara hacker (atau yang oleh **Paul Taylor** disebut sebagai *Computer Security Industry*) dan cracker (*Computer*

---

12 Eric S. Raymond, *The New Hacker's Dictionary*, MIT Press, versi elektronik dapat dijumpai di http://www-mitpress.mit.edu/seb/book-home/0262680920.htm

13 Shailen S. Mistry, *Hacker on the Net*, versi elektronik dapat dijumpai http://lis.gseis.ucla.edu/impact/196/Projects/Smistry/index.html

Underground) adalah masalah etika. Keduanya memiliki basis etika yang berbeda atau memiliki interpretasi yang berbeda terhadap suatu topik yang berhubungan dengan masalah *computing*. Selain masalah etika, masalah umur oleh **Paul Taylor** juga dipandang menjadi alasan yang membedakan pandangan atau interpretasi terhadap suatu topik. *Computer Security Industry* beranggapan bahwa *Computer Underground* masih belum memahami bahwa *computing* tidak sekedar permainan dan mereka (*Computer Underground*) harus melepaskan diri dari *playpen* (boks tempat bayi bermain).[14]

Hacker memiliki etika yang harus dipatuhi oleh setiap hacker, sedangkan cracker tidak memiliki (atau mempunyai interpretasi yang lain terhadap) etika ini. Etika Hacker (*The Hacker Ethic*) yang dimaksud adalah seperti yang terdapat dalam buku *Hackers: Heroes of the Computer Revolution*, karya **Steven Levy**, yaitu

a. Access to computers - and anything else which might teach you something about the way the world works - should be unlimited and total. Always yield to the Hands-On Imperatif.
b. All Information should be free
c. Mistrust Authority - Promote Decentralization
d. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position
e. You can create art and beauty on a computer
f. Computers can change your life for the better.

Selain etika yang dikemukakan oleh **Steven Levy** tersebut, ada juga etika hacker yang dikemukakan oleh **Loyd Blankenship** alias **The Mentor** yang tergabung dalam *Legion of Doom/Legion of Hackers*. Etika hacker yang dimaksud oleh **The Mentor** adalah sebagai berikut:

---

14 Paul Taylor sebagaimana dikutip oleh Budi Rahardjo, *Keamanan Sistem Informasi Berbasis Internet*, PT. Insan Komunikasi/Infonesia-Bandung, 2000, versi elektronik dapat dijumpai di http://budi.insan.co.id/book/handbook.pdf.

I. Do not intentionally damage *any* system.
II. Do not alter any system files other than ones needed to ensure your escape from detection and your future access (*Trojan Horses*, Altering Logs, and the like are all necessary to your survival for as long as possible.)
III. Do not leave your (or anyone else's) real name, real handle, or real phone number on any system that you access illegally. They *can* and will track you down from your handle!
IV. Be careful who you share information with. Feds are getting trickier. Generally, if you don't know their voice phone number, name, and occupation or haven't spoken with them voice on non-info trading conversations, be wary.
V. Do not leave your real phone number to anyone you don't know. This includes logging on boards, no matter how k-rad they seem. If you don't know the sysop, leave a note telling some trustworthy people that will validate you.
VI. Do not hack government computers. Yes, there are government systems that are safe to hack, but they are few and far between. And the government has inifitely more time and resources to track you down than a company who has to make a profit and justify expenses.
VII. Don't use codes unless there is *NO* way around it (you don't have a local telenet or tymnet outdial and can't connect to anything 800...) You use codes long enough, you will get caught. Period.
VIII. Don't be afraid to be paranoid. Remember, you *are* breaking the law. It doesn't hurt to store everything encrypted on your hard disk, or keep your notes buried in the backyard or in the trunk of your car. You may feel a little funny, but you'll feel a lot funnier when you when you meet Bruno, your transvestite cellmate who axed his family to death.
IX. Watch what you post on boards. Most of the really great hackers in the country post *nothing* about the system they're currently working except in the broadest sense (I'm working on a UNIX, or a COSMOS, or something generic. Not "I'm hacking into General Electric's Voice Mail System" or something inane and revealing like that.)
X. Don't be afraid to ask questions. That's what more experienced hackers are for. Don't expect *everything* you ask to be answered, though. There are some things (LMOS, for instance) that a begining hacker shouldn't mess with. You'll either get caught, or screw it up for others, or both.
XI. Finally, you have to actually hack. You can hang out on boards all you want, and you can read all the text files in the world, but until you actually start doing it, you'll never know what it's all about. There's no thrill quite the same as getting into your first

> system (well, ok, I can think of a couple of bigger thrills, but you get the picture.)[15]

Cracker tidak mempunyai niat atau kemauan untuk mengikuti etika itu. Ketidakmauan atau tidak adanya niat cracker untuk mematuhi etika hacker terbukti dengan aksi mereka yang telah merusak sistem komputer suatu perusahaan atau lawan politiknya, menyerang dan merusak situs-situs pemerintah atau pelayanan publik dan situs-situs yang memberikan layanan pendidikan dan penelitian.

Bagi hacker, akses ke komputer itu penting, sehingga tidaklah perlu dilakukan pembatasan untuk memperoleh akses itu. Akses ke komputer atau jaringan komputer adalah hak asasi setiap orang, dan untuk mewujudkan sikap hacker akses ke komputer atau jaringan komputer menjadi penting. Semua informasi adalah bebas, tetapi kebebasan itu tidak akan berarti tanpa adanya akses ke komputer. Seorang hacker meyakini bahwa komputer dan jaringan komputer merupakan wahana untuk melakukan tindakan atau perbuatan kreatif sekaligus dapat mengubah kehidupan ini menjadi lebih baik.

Salah satu wujud dari etika dan sikap hacker ini adalah apa yang diperlihatkan oleh **Richard M. Stallman**, hacker eks MIT. Ia mendirikan *Free Software Foundation* dan memungkinkan para hacker untuk memperoleh program bantu dengan gratis. Selain **Stallman**, banyak hacker yang menulis program-program kecil yang kemudian didistribusikan secara gratis sesuai kode

---

[15] The Mentor, *A Novice's Guide to Hacking*, edisi 1989, versi elektronik dapat dijumpai di http://www.geocities.com/dht_belgium/Legion_of_Doom.txt Lihat juga Legion of the Underground, *Hacking Guide*, versi elektronik dapat dijumpai di http://www.geocities.com/dht_belgium/lou_guide.txt

etik mereka. Salah satunya adalah **Linus Torvalds**, seorang mahasiswa Helsinki University, penemu program ***Linux***.[16]

Linux merupakan jawaban atas mahalnya harga sistem operasi UNIX komersial yang sangat berperan penting dalam aktivitas hacking. Mahalnya UNIX mendorong **Linus Torvalds** untuk menulis sistem operasi klon UNIX secara gratis (sebelumnya **Stallman** telah menjanjikan untuk menulis sistem operasi yang lebih murah dari UNIX, tetapi sampai terciptanya Linux, janji tersebut belum terwujud). Dengan bantuan *Free Software Foundation*, **Linus** berhasil menciptakan klon UNIX, yaitu Linux pada tahun 1992. Linux cukup populer di kalangan hacker sebagai alternatif UNIX dan karena penyebaran kode sumbernya dilakukan secara cuma-cuma, maka Linux mengalami perkembangan dalam wujud beberapa versi.

Kesalahan dalam menempatkan istilah hacker dan cracker tidak hanya dilakukan oleh media nasional tetapi juga oleh media internasional sehingga bagi mereka yang tidak memahami makna keduanya akan menyamakan saja artinya. Penggunaan atau penempatan istilah yang tidak sesuai ini akan menimbulkan kebingungan atau kesesatan dikalangan pembaca atau pendengarnya.

Kesalahan pengertian ini menyebabkan terjadinya salah tangkap pada operasi-operasi yang dilakukan oleh pihak kepolisian di Amerika Serikat. Sering terjadinya salah tangkap ini menyebabkan sekelompok hacker yang dipimpin oleh **Mitchell D. Kapor** dan **John Perry Barlow** mendirikan *Electronic Frontiers Foundation* (EFF) pada Juni 1990. Pendirian EFF ini bertujuan untuk

---

[16] Gede Artha Azriadi Prana, *op.cit*, hal. 33

memberikan bantuan hukum bagi orang-orang yang dirugikan oleh operasi-operasi yang salah sasaran termasuk hacker-hacker yang tidak bermotif kriminal.

Salah satu korban salah tangkap itu adalah **Loyd Blankenship** alias **The Mentor**. Ia yang terdaftar sebagai karyawan Perusahaan *Steve Jackson Games* pada saat itu tengah merancang sebuah produk permainan baru yang berjudul *Generic Universal Role Playing System - GRUPS Cyberpunk.* Produk permainan tersebut oleh agen-agen keamanan di Amerika Serikat dipandang sebagai buku petunjuk mengenai cara melakukan kejahatan komputer dan perusahaan *Steve Jackson Games* kemudian ditutup. Perusahaan *Steve Jackson Games* akhirnya memperoleh bantuan dari *Electronic Frontier Foundation* dalam menuntut petugas-petugas Secret Service atas penyitaan yang dialaminya.[17]

Setelah penangkapannya itu, **Loyd Blankenship** yang juga anggota *Legion of Doom* (saat ditangkap masih menjadi anggota kelompok *Racketeers*) menulis manifesto hacker sebagai wujud protes atas penangkapannya itu pada tahun 1986. Berikut manifesto hacker yang ditulisnya itu

> **The Conscience of Hacker**
>
> "This is our world now ... the world of the electron and the switch, the beauty of the baud. We make use of a service already exixting without paying for what could be dirt cheep if it wasn't run by profiteering gluttons, and you call us criminals. We explore ... and you call us criminals. We exist without skin color, without nationality, without religious bias ... and you call us criminals. You build atomic bomb, wage wars, murder, cheat, and lie to us and try to make us believe it is for our own good, yet we're the criminals.
>
> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never

[17] *Ibid.* hal. 32

> forgive me for. I am a hacker and this is my manifesto. You may stop this individual, but you can't stop us all ... after all, we're all alike."[18]

Cracker yang mempergunakan kemampuan hacking untuk melakukan kejahatan tidak selalu bernasib buruk setelah ditangkap oleh petugas keamanan. Mereka justru dapat memperoleh pekerjaan dengan mengajarkan teknik-teknik hacking kepada pihak keamanan dengan imbalan sejumlah uang tertentu ataupun kebebasan. Sebagai contohnya adalah **Neal Patrick** (anggota *414 Gang*), **Bill Landreth** (anggota *Inner Circle*) dan masih banyak lagi.

Dari penjelasan tersebut di atas dapat dipertegas bahwa penggunaan istilah hacker yang selama ini terjadi adalah salah kaprah karena mencampuradukkan makna kata hacker dengan cracker. Kesalahan dalam penyebutan istilah ini menyebabkan konstruksi makna yang berkembang di masyarakat menjadi tidak benar, dan konstruksi ini nampaknya sampai sekarang tetap ada dan terpelihara, terbukti dengan pemberitaan media yang masih menempatkan hacker sebagai pelaku cybercrime.

Vandal komputer atau bogus hacker muncul sebagai akibat dari tersebarnya informasi mengenai hacking dan keamanan komputer berupa kelemahan suatu sistem operasi atau hasil pemrograman. Kelompok Hacker dan Cracker tidak menyebut bogus hacker ini sebagai bagian dari mereka. Hacker atau cracker mempunyai kemampuan hacking melalui proses belajar yang tidak singkat, sedangkan bogus hacker hanya tahu sedikit tentang seluk beluk komputer. Ketika mereka (*bogus hacker*) bisa meng-hack sebuah situs, mereka

---

[18] *The Conscienscе of a Hacker*. ditulis oleh The Mentor, dimuat di Phrack vol 1 Edisi 7, file 3. Versi Indonesia dapat dilihat di situs kecoak elektronik, sebuah perkumpulan individu pengguna Internet di Indonesia, di http://www.k-elektronik.org/manifesto.html

akan menyombongkan diri dan bangga atas kemampuan menghacknya itu, sesuatu yang tidak dimiliki atau dihindari baik oleh hacker maupun cracker.

Meskipun pengertian dan pembedaan istilah hacker, cracker dan bogus hacker telah jelas, akan tetapi dalam perkembangannya peran dan pengertian dari hacker, cracker dan bogus hacker juga simpang siur. Perkembangan peran dan pengertian ini terjadi karena hacker yang seharusnya berwatak baik dengan alasan nasionalisme (baik nasionalisme terhadap negara, harta kekayaan maupun nama baik pribadi atau golongan) dapat berubah menjadi cracker.

Pergeseran peran dan pengertian ini dapat dilihat ketika situs pemerintah Indonesia dihack oleh *hacker Porto*. Para hacker Indonesia dengan alasan nasionalisme itu berusaha melakukan serangan balik dengan merusak situs milik gerakan pro kemerdekaan Timor-Timur yang bermarkas di Irlandia. Serangan balik ini menyebabkan kelumpuhan total pada situs yang dikelola oleh *Connect Ireland*.

Selain itu ada juga hacker yang menawarkan jasanya kepada publik untuk melakukan hacking terhadap sebuah situs dengan imbalan sejumlah uang atau sebaliknya menawarkan jasanya untuk menjadi pengaman pada situs yang berani menyewanya. Dari sini tampak bahwa istilah hacker dan cracker hampir tidak ada bedanya, sehingga untuk memahami kedua istilah itu dalam penulisan laporan ini harus dilihat konteks kalimatnya.

2. Kemampuan Yang Harus Dimiliki Oleh Seorang Hacker, Cracker dan Vandal Komputer atau Bogus Hacker

Menjadi hacker yang sejati memerlukan proses dan proses itu memakan waktu yang tidak sedikit. Pengetahuan yang didapat dari belajar untuk

menjadi hacker apabila dipraktekkan mengandung resiko, berupa rusak atau tidak berfungsinya komputer yang dipakai dan jika hal ini diteruskan, biaya yang dikeluarkan akan semakin besar. Untuk itu apabila ingin menjadi hacker sejati, belajarlah dengan mereka yang telah menjadi hacker atau mereka yang mengerti tentang bahasa pemrograman. Meskipun dengan belajar sendiri seseorang dapat menjadi hacker, tetapi prinsip-prinsip yang dipunyai dan dipegang teguh oleh hacker sejati tidak akan tersampaikan. Prinsip-prinsip tersebut memang dapat dipelajari, tetapi dengan belajar bersama orang yang menghayati makna dan berkomunikasi dengannya akan membuat pengertian yang timbul di dalam diri orang yang sedang belajar akan semakin sempurna.

Prinsip hacker tercermin dari sikap atau perilaku yang dimiliki dan dipertunjukkan olehnya. Seperti disebutkan di atas, perilaku yang tidak sesuai dengan prinsip-prinsip hacker atau menginterpretasikan prinsip itu secara lain akan menyebabkan orang tersebut tidak bisa disebut hacker, tetapi lebih tepat disebut cracker, bahkan mungkin vandal komputer atau bogus hacker. Jadi langkah untuk mengerti, menghayati, menjiwai dan meyakini prinsip-prinsip hacker itu memiliki posisi yang penting sebagai langkah awal untuk menjadi hacker.

Prinsip yang tercermin dalan sikap dan perilaku hacker itu penting, tetapi prinsip itu menjadi tidak penting jika tidak disertai dengan kemampuan. Sikap bukan pengganti kemampuan dan untuk menjadi hacker sejati ada seperangkat kemampuan untuk menggunakan seperangkat *tool* yang perlu dikuasai sebelum orang berfikir dan memanggilnya sebagai seorang hacker.[19]

---

[19] Eric S. Raymond, *op.cit.*

Seperangkat *tool* ini dalam perjalanan waktu terus mengalami kemajuan seiring dengan kemajuan yang dicapai dalam perkembangan komputer dan jaringan komputer. Cara mengikuti perkembangan itu bisa dilakukan dengan menghadiri (kalau bisa) setiap pertemuan antar hacker atau memantau lewat internet dan rajin mengikuti diskusi-diskusi mengenai suatu sistem operasi yang bisa dilakukan lewat *mailing list* serta eksperimen terhadap program-program atau sistem operasi yang sedang berkembang saat itu.

Perkembangan yang terjadi pada komputer dan jaringan komputer menyebabkan seperangkat *tool* yang lama menjadi kurang berguna, tetapi mengingat para pengguna jaringan komputer tidak selalu menggunakan teknologi komputer dan jaringannya yang terbaru maka *tool* lama tetaplah dapat digunakan. Misalnya dahulu keahlian pemrograman bahasa mesin termasuk yang harus dikuasai dan kemampuan HTML belum. Tetapi sejak maraknya World Wide Web yang berbasis HTML, maka kemampuan HTML menjadi keharusan untuk dikuasai.

Dari sekian banyak kemampuan yang harus dikuasai, beberapa hal yang saat ini betul-betul harus dipelajari dan kuasai untuk menjadi atau memiliki kemampuan sebagai hacker adalah:[20]

a. Pelajari pemrograman (*Learn how to program*)

   Ketika seorang hacker belajar tentang bahasa pemrograman, ia pasti akan belajar bagaimana menggunakan bahasa tersebut secara mahir dan lancar.[21]

---

[20] Disarikan dari Eric S. Raymond, *op.cit*, dilengkapi hasil wawancara dengan Budi Rahardjo dari Pusat Antar Universitas Bidang Mikroelektronika ITB pada tanggap 30 April 2001, Basuki dan Afan Basalamah dari CNRG PAUME ITB pada tanggal 28 dan 30 April 2001.

[21] Belajar membuat program adalah seperti belajar menulis dalam bahasa alamiah. Cara terbaik untuk melakukannya yaitu dengan membaca tulisan yang dibuat oleh para ahli menulis, membuat tulisan sendiri sedikit, membaca lebih banyak lagi, menulis lebih banyak dan mengulanginya sampai tulisan yang dibuat itu mempunyai kekuatan dan kemahiran menggunakan kata seprti

Tetapi sejak awal harus sudah ditekankan bahwa hacking tidak sekedar membuat bom e-mail, mengirim e-mail sampah atau merusak situs tertentu. Pemrograman merupakan keahlian hacking yang fundamental. Keahlian dalam pemrograman digunakan untuk mengetahui atau mendeteksi kelemahan dari sistem operasi yang dipakai target atau sasaran hacking. Mereka yang belum mengerti bahasa pemrograman (pemula) disarankan untuk mempelajari dan menggunakan ***Phyton.*** [22] Bahasa pemrograman Java juga bagus untuk diperlajari, tetapi lebih sulit dari Phyton, tetapi pembuatan kodenya lebih cepat dibandingkan Phyton. Java menjadi bahasa kedua yang paling bagus dalam pemrograman.[23]

Jika ingin serius dalam mempelajari pemrograman, pada akhirnya orang tersebut harus belajar bahasa C, bahasa inti sistem operasi UNIX (meskipun C bukan bahasa pertama yang sebaiknya dipelajari), Linux dan macam-macam aplikasi lainnya. Bahasa Pemrograman C++ sangat erat berhubungan dengan bahasa C, jika telah mengetahui satu bahasa, mempelajari bahasa lainnya tidaklah sulit. Bahasa pemrograman C++ digunakan untuk berbagai macam aplikasi. C++ merupakan pengembangan dari bahasa C atau dengan

---

tulisan-tulisan yang diteladani. Dahulu sulit mencari kode yang baik untuk dibaca karena hanya sedikit program-program besar yang terdapat dalam bentuk source untuk bisa dibaca dan dimainkan oleh hacker-hacker pemula. Sekarang kondisinya jauh berbeda, software open-source, *tool* pemrograman dan sistem operasi (semua dibuat oleh hacker) banyak dan mudah didapat. Eric S. Raymond, *Ibid.*

22 Phyton memiliki rancangan yang bagus, dokumentasinya juga bagus dan cukup mudah bagi pemula. Meski menjadi bahasa pertama bukan berarti Phyton hanya mainan, Phyton amat ampuh dan fleksibel dan cocok untuk proyek-proyek besar. Eric S. Raymond, *Ibid.*

23 Namun perlu diingat bahwa dengan satu atau dua bahasa pemrograman saja tidak akan mencapai tingkat kemampuan seorang hacker atau bahkan seorang programmer, masih perlu belajar cara memandang pemrograman secara umum, tidak bergantung pada satu atau dua bahasa manapun. Untuk menjadi hacker sejati, Seseorang (yang berminat menjadi hacker) perlu mencapai tahap di mana orang tersebut dapat mempelajari bahasa baru dalam beberapa hari dengan menghubungkan apa yang ada di manual dengan apa yang anda ketahui. Hal ini berarti orang tersebut perlu mempelajari beberapa bahasa yang jauh berbeda satu dengan yang lainnya.

kata lain bahasa C tercakup dalam C++ atau C++ merupakan *superset* dari C. Bahasa pemrograman C++ merupakan bahasa yang cukup andal karena kecepatan eksekusinya.[24]

Bahasa lain yang terutama penting untuk hacker antara lain Perl dan LISP. Perl patut dipelajari untuk kebutuhan praktis sedangkan LISP patut dipelajari karena akan memberikan pengalaman membuka pikiran, jika orang tersebut memahaminya.[25] Akan lebih baik lagi jika dipelajari juga bahasa pemrograman Basic dan Assembly.

Paling baik sebetulnya mempelajari semuanya (Phyton, Java, C, C++, Perl, LISP, Basic dan Assembly). Selain merupakan bahasa-bahasa terpenting dalam hacking, masing-masing mewakili cara pendekatan pemrograman yang berbeda dan tiap bahasa akan memberi kepada orang tersebut pelajaran-pelajaran berharga. Pemrograman merupakan keahlian yang kompleks, buku dan kursus saja tidak akan membuat orang tersebut menjadi seorang programer (banyak, mungkin hampir semua hacker terbaik belajar mandiri). Orang akan menjadi programer dengan membaca kode dan menulis kode.

Seiring dengan perkembangan yang terjadi maka belajar sistem operasi Linux menjadi penting. Perkembangan Linux (merupakan klon dari UNIX)

---

[24] Kelebihan C++ dibandingkan dengan C adalah dukungan untuk pemrograman berorientasi pada objek alias object-oriented programming (OOP) yang berguna untuk pemrograman besar dan memungkinkan pewarisan sehingga program yang relatif sama dengan program yang pernah dibuat sebelumnya tidak perlu dikode ulang. Ada berbagai macam kompiler dari C++ yang dapat digunakan dan yang terkenal adalah Borland C++. Kompiler versi komersialnya berbasis grafis dan punya fasilitas yang banyak, mulai dari debugger, help yang lengkap dan masih banyak lagi. Lengkapnya fasilitas yang ada pada C++ menyebabkan bahasa pemrograman ini dapat dipelajari tanpa menggunakan buku tambahan.

[25] Perl dipakai amat meluas untuk halaman web aktif dan untuk administrasi sistem, jadi meskipun nantinya orang tersebut tidak akan membuat program dalam Perl, mereka sebaiknya belajar cara membaca Perl. Dengan mempelajari LISP, orang tersebut akan menjadi seorang programer yang lebih baik, meskipun dalam kenyataan akan jarang memakainya.

sangat cepat karena didistribusikan secara gratis dan terbuka untuk didiskusikan mengenai kelemahan-kelemahan yang ada pada versi terbarunya.

Mempelajari bahasa pemrograman dapat saja dilakukan oleh orang awam mengingat perkembangan penerapan komputer di bidang bisnis. Menurut **Rendra T. Surya** dengan mengutip pendapat **Peter Norton** ada beberapa alasan yang menyebabkan orang awam perlu belajar bahasa pemrograman, yaitu:[26]

1) Perangkat lunak bahasa (pembuatan program) versi sekarang semakin canggih, namun cara membuatnya semakin mendekati cara kerja/berfikir manusia umumnya. Dengan hanya berbekal logika yang baik dan memahami persoalan yang akan diselesaikan oleh program, siapapun pemakai komputer yang berminat bisa mengusai teknik-teknik pemrograman yang berorientasi end-user tersebut.
2) Betapapun canggihnya software-software paket (aplikasi) karena sudah dibuat sebelumnya maka hanya dapat menyelesaikan persoalan yang bersifat umum dan standar. Di sisi lain banyak persoalan khusus yang sulit diotomatisasi (dikomputerisasi) dengan software paket tersebut sehingga mau tidak mau end-user computer harus mengutak-atik ke software paket tersebut agar memiliki kemampuan tambahan yang diinginkan.
3) Meskipun perusahaan skala menengah dan besar pasti memiliki bagian atau unit yang khusus menangani komputer, namun semakin hari semakin nyata adanya tuntutan independensi dari end-user computer.

b. Cari, pelajari dan jalankan salah satu versi UNIX open-source (*Get one of the open-source UNIXes and learn to use and run it*)

UNIX adalah sistem operasi yang dibuat oleh AT & T Bell Laboratories melalui dua karyawannya **Ken Thompson** dan **Dennis Ritchie.** UNIX memungkinkan komputer untuk menangani banyak pengguna dan program

---

[26] Rendra T. Soerya, *Siapa Perlu Belajar Pemrograman*?, PCplus No. 15/II/06 Februari 2001, hal. 15.

secara simultan. Seiring dengan munculnya komputer pribadi maka muncul pula UNIX to UNIX CoPy (UUCP). UUCP merupakan suatu program yang berjalan di bawah sistem operasi UNIX yang memungkinkan sebuah sistem UNIX untuk mengirimkan file-file ke sistem UNIX yang lain lewat jalur telepon dial up. UUCP sering digunakan untuk menjelaskan mengenai suatu jaringan internasional yang yang menggunakan protokol UNIX untuk menyampaikan berita-berita dan e-mail. Sistem operasi UNIX untuk komputer dinilai terlalu mahal sebuah komputer pribadi sehingga perlu dicari klon atau turunannya, yaitu Linux atau BSD (Berkeley Software Distribution). BSD merupakan implementasi dari sistem operasi UNIX dan utilitasnya yang dibentuk serta disebarkan oleh Universitas California di Berkeley. BSD biasanya didahului dengan nomor versi distribus, misalnya 4.3. BSD yang berarti merupakan versi 4.3. dari distribusi Berkeley UNIX.

Langkah terpenting bagi seorang pemula untuk mendapatkan kemampuan hacker adalah mendapatkan satu salinan sistem operasi Linux atau salah satu UNIX BSD, menginstalnya di komputer pribadi (jika punya) dan menjalankannya. Di dunia ini ada banyak sistem operasi selain UNIX, tetapi sistem-sistem operasi tersebut didistribusikan dalam program jadi (binary), kodenya tidak bisa dibaca, sehingga sistem operasi tersebut tidak bisa dimodifikasi. Belajar hacking di DOS atau Windows atau MacOS adalah bagaikan belajar menari dengan seluruh tubuh digips (*to learn to dance while wearing a body cast*).[27]

---

[27] Eric Raymond, *op.cit.*

Lagipula UNIX-lah sistem operasi Internet, meskipun bisa belajar menggunakan internet tanpa mengenal UNIX. Seseorang tak akan mempu menjadi hacker Internet tanpa memahami UNIX. Untuk alasan inilah budaya hacker saat ini cukup berat ke UNIX (ini tidak selalu benar, beberapa hacker jaman dahulu tidak menyukai kenyataan ini, tetapi simbiosis antara UNIX dan Internet telah menjadi kuat sehingga bahkan otot Microsoft pun tak mampu membengkokkannya). Jadi buatlah sistem UNIX (meskipun bisa juga digunakan Linux dan menjalankannya bersama DOS/Windows di mesin yang sama). Pelajari UNIX dan jalankan. Berhubungan dengan internet melalui UNIX, baca kodenya dan modifikasi. Seseorang (yang ingin menjadi hacker dan belajar UNIX) akan bersenang-senang dan orang tersebut akan mendapat pengetahuan lebih dari yang anda sadari sampai kemudian ketika mengenang kembali orang tersebut telah seorang hacker ahli (*master hacker*).

c. Pelajari cara menggunakan World Wide Web dan cara menulis HTML (*Learn how to use the World Wide Web and write HTML*)

Kebanyakan hasil budaya hacker bekerja di belakang layar tanpa diketahui orang banyak, membantu mengoperasikan pabrik, kantor dan universitas tanpa pengaruh yang jelas pada cara hidup non hacker. Web adalah satu kekecualian, bahkan para politisipun mengakui bahwa barang mainan hacker yang besar dan berkilauan ini telah mengubah dunia. Untuk satu alasan ini saja seseorang yang belajar atau ingin menjadi hacker perlu mempelajari pengoperasian Web. Maksudnya lebih dari sekedar cara menggunakan browser, tetapi mempelajari cara menulis HTML, bahasa *mark up* Web.

Apabila orang belum menguasai pemrograman, lewat menulis HTML orang tersebut akan diajari beberapa kebiasaan mental yang akan membantunya belajar pemrograman, jadi buatlah home page. Hanya dengan membuat home page tidak akan membuat orang menjadi (bahkan dekat pun tidak) seorang hacker. Web penuh dengan *home page*. Kebanyakan hanyalah kotoran tanpa arti, tanpa isi, kotoran yang tampak indah, tetapi tetap kotoran. Agar bermanfaat sesuai dengan sikap hacker yang selalu memberi, halaman home page yang dibuat itu harus mengandung *content*, harus menarik dan berguna bagi hacker lain.

Kemampuan pemrograman dan hacking tidak serta merta menjadikan mereka menjadi seorang hacker. Apa yang bisa diberikan kepada orang lain (berupa hasil kreativitasnya) dan kemampuan untuk memecahkan masalah-masalah yang dihadapi oleh banyak orang (terutama yang berkaitan dengan masalah pemrograman dan hacking) dapat dijadikan ukuran untuk menilai apakah seseorang itu layak atau tidak disebut sebagai hacker. Penilaian itu tidak dilakukan atau diberikan oleh masyarakat umum, tetapi dilakukan atau diberikan oleh kalangan sejawat, yaitu para hacker.

Dalam permainan hacker, seorang hacker menjaga nilai terutama lewat pandangan hacker lain terhadap kemampuannya (inilah sebabnya seorang hacker belum benar-benar menjadi hacker sampai hacker-hacker lain dengan konsisten menyebut hacker tersebut sebagai seorang hacker). Kenyataan ini dikaburkan oleh citra hacker sebagai pekerjaan menyendiri, juga oleh tabu budaya hacker yang kini perlahan-lahan menghilang namun masih tetap kuat, yang tidak mengakui bahwa ego atau pengesahan dari luar berpengaruh pada motivasi

seseorang. Tegasnya dunia hacker merupakan apa yang disebut oleh para antropolog sebagai budaya memberi. Kedudukan dan reputasi tidak diperoleh dengan menguasai orang lain, atau dengan menjadi seseorang yang cantik atau dengan memiliki sesuatu yang tidak dimiliki orang lain, tetapi dengan memberikan sesuatu, tepatnya dengan memberikan waktu, kreativitas dan hasil dari kemampuan yang dimilikinya.[28]

Pada dasarnya ada lima hal yang bisa dilakukan seseorang agar dinilai sebagai hacker dan dihormati oleh sesama hacker, yaitu:[29]

a. Menulis *software open-source* (*Write open-source software*)

   Pertama yang paling inti dan tradisional adalah menulis program yang dipandang berguna atau mengasyikkan oleh hacker lain, kemudian memberikan source programnya untuk digunakan oleh seluruh komunitas hacker. Dahulu karya semacam itu disebut software bebas (*free software*), tetapi istilah ini memusingkan banyak orang karena mereka tidak tahu apa arti yang tepat dari free, sehingga sekarang banyak yang lebih menyukai istilah *software open-source*. Para dewa[30] yang dipuja di dunia hacker yaitu mereka yang telah menulis program besar yang berkemampuan tinggi dan dibutuhkan di mana-mana, lalu memberikan program ini cuma-cuma dan sekarang program ini telah dipakai setiap orang.

---

[28] *Ibid.*

[29] *Ibid.* Bandingkan dengan Gede Artha Azriadi Prana yang menyebutkan ada empat jenis aktivitas yang dipandang mampu menaikkan prestasi seorang hacker sejati, yaitu:
   a. Menulis dokumen tentang hacking
   b. Menciptakan program yang bermanfaat
   c. Aktif menyumbangkan pengetahuan dalam forum hacking
   d. Ikut berpartisipasi dalam mencegah kejahatan komputer.

[30] Para dewa atau demigod adalah hacker yang telah memiliki pengalaman bertahun-tahun, memiliki reputasi kelas dunia dan berperan penting dalam pengembangan rancangan, *tool* atau game yang dipakai atau dikenal oleh minimal lebih dari separuh komunitas hacker (dari Jargon File 4.1.2).

b. Membantu menguji dan men-*debug software open-source* (*Help test and debug open-source software*)

Hacker yang berjasa adalah hacker yang bertahan menggunakan dan men-*debug software open-source.* Tanpa terhindarkan para hacker harus menghabiskan sebagaian besar waktu pengembangan software dalam tahap *debugging*, karena itu setiap penulis *software open-source* yang sehat akan berpendapat bahwa penguji beta yang baik atau *good beta-testers* (yang tahu bagaimana menjelaskan gejala masalah dengan jelas, bagaimana melokalisir masalah, mampu mentolerir bug di rilis cepat dan bersedia menjalankan beberapa rutin diagnostik sederhana) itu amat sangat berharga. Bahkan satu saja penguji beta sudah mampu membantu menjadikan tahap *debugging* dari mimpi buruk panjang yang melelahkan menjadi hanya gangguan yang justru menyehatkan. Untuk seorang pemula belajar menguji dan men-debug ini dapat dilakukan dengan mencoba mencari program yang sedang dalam tahap pengembangan yang menarik baginya. Dari sini hacker pemula secara alamiah akan meningkat dari membantu menguji program ke membantu memodifikasi program.

c. Menerbitkan informasi yang bermanfaat (*Publish useful information*)

Selain hal tersebut di atas, hal lain yang perlu dilakukan adalah mengumpulkan dan menyaring informasi-informasi menarik dan berguna ke dalam halaman Web atau dokumen seperti FAQ (Frequently Asked Question, daftar jawaban pertanyaan-pertanyaan yang sering diajukan orang), dan membuat dokumen-dokumen ini mudah di dapat orang.

Pemeliharaan FAQ teknis yang besar-besar juga mendapatkan hormat hampir seperti para penulis software open-source.

d. Membantu terus berjalannya infrastruktur (*Help keep the infrastructure working*)

Budaya hacker dijalankan oleh relawan. Banyak sekali pekerjaan yang dibutuhkan namun bukan pekerjaan yang agung, yang harus dilakukan agar semua tetap berjalan, melakukan administrasi mailing list, menjadi moderator newsgroup, memelihara situs archive software yang besar, mengembangkan dokumen-dokumen Request for Comment (RFC) serta standar teknis lainnya. Mereka yang melakukan hal-hal seperti itu dengan baik juga dihormati, karena orang tahu bahwa pekerjaan seperti ini menghabiskan banyak waktu dan tidak kalah mengasyikkan dibanding bermain dengan kode. Melakukan pekerjaan seperti ini menunjukkan bahwa seseorang memiliki dedikasi.

e. Mengabdi kepada budaya hacker itu sendiri (*Serve the hacker culture itself*)

Seseorang dapat mengabdi dan menyebarluaskan budaya hacker (lewat, misalnya menulis panduan tepat bagi pemula tentang cara menjadi seorang hacker). Tetapi hal itu tidak mudah untuk dilakukan kecuali telah berkecimpung cukup lama dan menjadi figur yang cukup terkenal di salah satu dari empat hal sebelumnya. Budaya hacker tidak persis memiliki pemimpin, tetapi memiliki pahlawan, ketua suku, sejarawan dan para juru bicara. Jika seseorang telah cukup lama berada di medan tempur, orang tersebut dapat saja memperoleh salah satu dari jabatan-jabatan ini. Tetapi sebagai peringatan adalah bahwa hacker tidak mempercayai ego ketua suku

yang terlampau mencolok, jadi berbahaya jika seseorang terlalu terlihat untuk berusaha menjadi terkenal. Cara yang benar seharusnya yaitu dengan memposisikan diri sedemikian rupa sehingga jabatan tersebut jelas telah dapat dicapai, kemudian bersikap rendah hati dan ramah sehubungan dengan kedudukan yang diperoleh tersebut.

Selain kelima hal tersebut di atas, seorang hacker akan memiliki prestasi dan prestise yang tinggi apabila ia mempunyai kemampuan untuk mendayagunakan komputer atau peralatan yang sederhana yang hasilnya melampaui kemampuan aslinya. Hacker dengan perangkat lunak yang dipakai dapat dan mampu melampaui batasan yang tak dapat dilewati pemakai biasa. Para hacker menilai hacker lain murni berdasarkan keahlian. Jenis kelamin, usia, pekerjaan, status sosial ekonomi, suku bangsa, agama, pandangan politik dan semacamnya tidak menjadi pertimbangan dalam menentukan posisi seorang hacker di mata hacker lain.

Untuk menjadi cracker atau vandal komputer atau bogus hacker tidaklah serumit menjadi hacker dengan segala atribut yang harus dipahami dan diyakini. Cracker dapat menyalahgunakan kemampuannya hackingnya untuk melakukan kejahatan. Perbuatan ini bertentangan dengan sikap, kode etik dan budaya hacker itu sendiri sehingga meskipun mereka memiliki kemampuan yang sama dengan hacker tidak dapat disebut sebagai hacker. Berbeda halnya dengan menjadi seorang vandal komputer atau bogus hacker yang tidak perlu memiliki kemampuan seperti seorang hacker atau cracker. Syarat untuk menjadi bogus hacker ini adalah bisa atau mampu menggunakan komputer, baik yang dipakai

untuk jaringan lokal (*Local Area Network/LAN*) maupun untuk *wide area network* (WAN/internet).

Kemampuan melakukan hacking bagi bogus hacker dapat diperoleh dari informasi atau berita yang disebarluaskan oleh hacker melalui media cetak maupun elektronik. Selain melalui media tersebut, informasi mengenai kelemahan suatu sistem atau program juga dapat diperoleh jika mengikuti diskusi di internet atau *mailing list*, atau membuka situs yang menyediakan layanan eksploitasi kelemahan sistem operasi tertentu.[31]

Dengan demikian untuk menjadi bogus hacker sangat mudah, tidak harus mengerti dan menguasai bahasa pemrograman atau sistem operasi atau dengan kata lain kemampuan yang dimiliki oleh bogus hacker adalah kemampuan kalengan atau instant karena kemampuan yang dimilikinya itu adalah program jadi yang telah dibuat oleh para hacker sehingga bogus hacker tinggal mengeksploitasi saja. Dari hal tersebut sangat dimungkinkan seorang bogus hacker melakukan hacking terhadap suatu situs yang menggunakan sistem operasi UNIX atau Linux atau Windows tanpa ia sendiri mengetahui apa itu UNIX, Linux atau Windows.

3. Tahap-tahap Hacking

Kemampuan hacking bagi seorang hacker atau cracker bukanlah kemampuan yang diperoleh secara singkat atau instant. Proses belajar dan diskusi dengan kalangan hacker adalah kata kunci untuk memiliki kemampuan

---

[31] Seorang bogus hacker yang aktif dalam diskusi mailing list atau rajin membuka situs-situs yang menyediakan layanan seperti itu akan memiliki lebih banyak informasi mengenai kelemahan sistem operasi dan hal tersebut meningkatkan kemampuan hackingnya, bahkan dapat pula meningkatkan statusnya menjadi hacker atau cracker jika ia mempunyai kemauan dan kemampuan mempelajari bahasa pemrograman..

itu. Kemampuan itu juga tidak berarti apabila tidak pernah digunakan atau dieksploitasi. Penguasaan bahasa pemrograman, sistem operasi dan eksperimen akan semakin meningkatkan kemampuan hacker dalam masalah hacking.

Seorang hacker atau cracker apabila hendak melakukan hacking tidak dilakukan secara sembarangan, artinya ada motif atau niat tertentu dibalik hacking itu. Peralatan untuk melakukan hacking juga sangat penting untuk diperhatikan. Untuk melakukan hacking, seorang hacker dapat menggunakan komputer sederhana atau minimal yang bisa dipakai untuk mengakses internet meskipun semakin baik atau tinggi kemampuan komputer yang dipakai akan semakin baik proses dan hasilnya. Hal ini tidak bisa terlepas dari ciri atau sifat hacker yang selalu berusaha untuk melakukan sesuatu yang melebihi kemampuan aslinya (dalam hal ini kemampuan komputer itu).

Untuk melakukan aksinya, seorang hacker atau cracker cukup menggunakan komputer PC/XT dengan kapasistas minimal 268, 1Mbyte dan 40 Mbyte Harddisk, modem dan saluran telepon. Dapat juga menggunakan komputer dengan spesifikasi hardware yang dibutuhkan adalah PC 386 DX ke atas (mampu menjalankan MS-Windows pada mode enchanced) dengan RAM 4 MB atau lebih (disarankan 8 MB), Disk Drive 1.44 MB HD, 3,5" dan 1.2 MB 5.1/4", Harddisk, Mouse, dengan sistem operasi Windows 3.1 (minimal) dan MS-DOS versi 5.0. Dengan komputer seperti itu seorang hacker mampu untuk melakukan hacking terhadap suatu sistem komputer yang mempunyai kualifikasi hardware dan software yang lebih tinggi atau lebih baik.

Selain motif atau niat dan komputer yang dipakai, maka langkah atau tahap yang harus dilalui oleh seorang hacker untuk melancarkan aksinya adalah sebagai berikut:[32]

a. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran.

   Pengetahuan mengenai sistem operasi yang dipakai ini penting karena akan membantu hacker dalam mengeksploitasi kelemahan sistem operasi target sasaran. Para hacker biasanya menggunakan UNIX atau berbagai variannya seperti *RedHat, FreeBSD, Slackware* maupun *OpenBSD*, meski demikian banyak juga program hacker yang ditulis untuk Windows bahkan DOS. Tetapi hacker yang benar-benar serius menggunakan UNIX atau Linux, karena fasilitas atau perintah untuk jaringannya lebih baik.

   Cara memperoleh informasi mengenai sistem operasi apa yang dipakai dalam jaringan komputer dapat diperoleh dari orang dalam, melalui pemberitaan di media atau dengan menghubungi nomor telepon perusahaan atau kantor yang hendak dituju. Jika nomor yang ditelpon itu memberikan *sinyal carrier* berarti nomor telepon itu terhubung ke modem komputer yang berarti pula perusahaan itu terhubung ke internet.

   Cara yang lebih mudah adalah dengan menggunakan satu unit komputer, akses ke internet, telnet dan untuk mempermudah atau memperlancar dapat

---

[32] Penjelasan lebih lengkap dapat dilihat pada Gede Artha Azriadi Prana, op.cit, hal. 45-65 ataupun dalam Legion of the Underground, *Hacking Guide*, versi elektronik dapat dijumpai di http://www.geocities. com/dht_belgium/lou_guide.txt. maupun dalam The Mentor, 1989, *A Novice's Guide to Hacking*, versi elektronik dapat dijumpai di http://www.geocities.com/dht_belgium/Legion_of_Doom.txt. Lihat juga Budi Rahardjo, Sistem Keamanan ..... *op.cit.*

digunakan program khusus seperti *prefix scanner, port scanner, Daemon Dialer* atau *War Dialer*.

Cara lainnya adalah dengan mencari sasaran di antara komputer-komputer host yang ada. Jadi yang di cari saat ini bukanlah komputernya, tetapi pintu masuk (*port*) yang bisa dimanfaatkan dalam sistem operasi komputer itu. Port atau pintu masuk ini berupa jalur-jalur keluar masuknya data dari dan ke suatu komputer. Pengaksesan komputer melalui *port* disebut *port surfing.* Pencarian port dapat lakukan dengan program khusus yang disebut *port scanner*, seperti *Rebellion, PartPro* dan *PortScanner. Port scanner* adalah suatu alat yang berfungsi untuk men-scan berbagai macam port dalam suatu client dan mengompilasi suatu daftar port atau alamat IP yang terbuka. Dari port yang terbuka dalam suatu sistem client itulah hacker bisa masuk ke dalamnya. Port-port yang sering terbuka misalnya port 23 (telnet), 43 (whois), 79 (finger), 25 (Simple Mail Transfer Protocol) dan sebagainya. Daftar port yang memuat port secara lengkap bisa diperoleh di mana-mana, misalnya dokumen RFC (Request For Comment) 1700, atau dari buku-buku yang membahas Internet secara teknis.

Servis-servis yang sering terdapat ini kemudian dapat digunakan untuk mengumpulkan informasi lebih jauh tentang host yang akan dijadikan sasaran. Servis yang paling umum dipakai adalah *finger. Finger* adalah servis umum bagi sistem operasi UNIX dan juga Windows (Finger23) merupakan perintah yang dapat menampilkan informasi mengenai seorang pemakai jaringan. Jika seseorang menjalankan program *finger client* untuk mencari keterangan tentang seseorang atau perusahaan di suatu sistem

tertentu, maka program *finger client* itu akan mengirimkan permintaan ke *finger daemon* ke sistem tertentu itu.

Daemon adalah program yang ditempatkan sebagai penunggu port-port pada host di Internet, yang bertugas menjalankan perintah-perintah dari luar secara otomatis, misalnya *mailer daemon, finger daemon. Finger daemon* ini kemudian akan mengirimkan informasi yang diminta ke orang tersebut. Informasi yang dikirim itu bisa berbeda-beda tergantung konfigurasi sistem tersebut dan yang paling umum ditampilkan misalnya login name, waktu login terakhir, waktu logout dan nama pemakai. Finger juga dapat digunakan untuk melihat daftar pemakai dalam suatu sistem. Dalam hal ini yang difinger adalah hostnya, bukan nama pemakai secara spesifik. Untuk alasan keamanan, banyak perusahaan atau badan hukum yang menonaktifkan finger daemon pada sistem mereka.

Selain hal tersebut di atas, seorang hacker juga memerlukan pengetahuan tentang *whois, nslookup, ping* dan *traceroute* untuk mengetahui suatu sistem operasi komputer di target sasaran. *Whois* biasanya digunakan untuk mencari nama-nama domain yang ada di internet, tetapi dapat juga digunakan untuk mencari informasi berharga tentang suatu server. *Nslookup* digunakan untuk melihat (*look up*) alamat dari nama domain daru suatu alamat Internet Protocol (*IP address*). Ping adalah suatu perintah pengiriman suatu paket yang berisi sejumlah byte dari suatu client ke client yang lain sampai kembali ke si pengirim sedangkan *traceRoute* adalah suatu perintah yang bekerja seperti ping, tetapi ia akan menunjukkan masing-masing router

yang dilewati dan melewati client tersebut. *TraceRouter* biasanya diperlukan untuk melacak komputer yang berada dalam sistem jaringan.

b. Menyusup atau mengakses jaringan komputer target sasaran.

Untuk masuk atau mengakses jaringan komputer target sasaran dapat dilakukan dengan menaklukkan atau menipu sistem pengaman yang ada pada jaringan komputer. Ada beberapa cara untuk menembus sistem pengaman yang ada pada jaringan komputer, diantaranya adalah *social engineering*, menebak dan memecah password, menyadap password, mengeksploitasi kelemahan pada sistem sasaran dan *trashing*.

Social engineering atau rekayasa sosial atau *con* adalah cara untuk menyusup ke dalam jaringan komputer yang dilakukan oleh seseorang yang berpura-pura menjadi seorang pekerja atau karyawan yang kehilangan password atau gagal mengakses komputer kerjanya sehingga nantinya akan diberi password baru. Cara yang paling umum adalah melalui telepon, dengan berbekal kecepatan berfikir, pengetahuan, kemampuan menyamarkan suara (dengan alat bantu pengubah suara). Dapat juga dilakukan melalui pos yaitu dengan berpura-pura menjadi sebuah perusahaan yang sedang mengadakan survei dengan mengirimkan daftar isian pada orang-orang yang menjadi sasarannya. Data-data penting dapat diambil dan data tersebut dapat digunakan untuk sarana *social engineering* melalui telepon.

Menebak dan memecah password dapat dilakukan dengan berbagai cara, seperti menebak kombinasi *username* dan password (seperti nama lengkap, nama orang tua, pacarnya, tokoh idola, binatang peliharaan, tempat dan/atau waktu kelahiran, nama acara favorit, dan sebagainya) dalam sistem yang

dijadikan sasaran. Cara ini kurang efektif karena sekarang orang dapat menebak password dengan menggunakan program pemecah password yang dilakukan dengan menyusun sebuah daftar kata yang sering dipakai atau digunakan orang. Program pemecah password ini akan mengkombinasikan kata-kata dalam daftar itu hingga mendapatkan kombinasi yang sesuai. Ada juga program yang dapat melakukan seluruh kombinasi karakter yang mungkin, baik huruf, angka maupun karakter yang lain. Metode ini dinamakan *brute forcing cracking*. Macam-macam *brute forcing* ini antara lain *crack* (UNIX), *viper* (perl script) dan *cracker jack* (DOS). *Crack* yang digunakan untuk sistem operasi UNIX merupakan program untuk menduga atau memecahkan *password* dengan menggunakan sebuah atau beberapa kamus (dictionary). Program crack melakukan *brute forcing* cracking dengan mencoba mengenkripsi sebuah kata yang diambil dari kamus dan kemudian membandingkan hasil enkripsi dengan password yang akan dipecahkan. Bila belum cocok maka akan dilakukan *brute forcing* lagi dengan mengambil kata selanjutnya.

Penggunaan metode menebak password memiliki ekses yang cukup jelek berupa jumlah kegagalan login yang tinggi sebagai akibat kombinasi yang salah sebelum kombinasi yang sesuai ditemukan, terutama pada penerapan metode *brute forcing*. Jumlah login yang gagal selalu dicatat dalam *log system* dan log ini hampir pasti diperiksa oleh administrator sistem secara rutin. Bisa saja terjadi pada saat pembobolan terjadi, administrator sedang melakukan *back up* atas seluruh data dan sistem operasi sehingga oleh administrator dapat diketahui pembobolan sedang berlangsung.

Pemilihan kata-kata untuk digunakan sebagai password perlu perhatian yang khusus, karena menggunakan kata-kata yang umum dapat dengan mudah dijebol oleh para cracker. Berikut daftar atau hal-hal yang sebaiknya tidak digunakan sebagai password:

1) Menggunakan namanya sendiri, nama isteri atau suaminya, nama anaknya atau nama kawan atau pacar/kekasihnya
2) Menggunakan nama atau merk komputer yang digunakan
3) Menggunakan nomor telepon atau plat nomor kendaraan yang dipunyai atau dipakai
4) Menggunakan tanggal, bulan dan tahun kelahiran
5) Menggunakan alamat rumah atau sekolah atau tempat kerja
6) Menggunakan tempat yang terkenal (yang menjadi favoritnya terutama)
7) Menggunakan kata-kata yang terdapat dalam kamus (baik Indonesia maupun Inggris)
8) Menggunakan password dengan karakter yang sama diulang-ulang
9) Menggunakan nama aktor atau aktris favorit, atlet olah raga idola dan binatang peliharaan.
10) Hal-hal tersebut di atas ditambah satu angka.[33]

Selain program menyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga progam penyerang yang sifatnya melakukan pencurian atau penyadapan data dan/atau password. Untuk menyadap data dan/atau ***menyadap password*** dapat dilakukan dengan berbagai cara dan cara yang umum adalah dengan menyadap dan memeriksa paket-paket data yang lalu

---

[33] Budi Rahardjo, *op.cit*, hal. 54.

lalang dalam suatu jaringan (lazim disebut *sniffing* atau *packet monitoring*). *Sniffing* ini sangat berbahaya karena dia dapat digunakan selain untuk menyadap password juga bisa digunakan untuk menyadap informasi yang sensitif (merupakan serangan terhadap aspek privacy). *Sniffing* (mengendus) biasanya dilakukan terhadap paket-paket yang dikirim dalam bentuk teks biasa (tidak terenkripsi). Praktek *sniffing* yang lebih maju dibantu oleh sebuah *protocol analyzer*, yang untuk membaca paket data yang dibungkus protokol tertentu. Pemeriksaan paket-paket data dalam suatu jaringan sebenarnya adalah juga praktek-praktek yang bermanfaat di kalangan administrator sistem untuk mengawasi gejala-gejala awal penyusupan. Sebuah program pemonitor paket dapat ditugaskan untuk mencari paket-paket yang berisikan kata-kata kunci semacam password, login dan sebagainya, lalu menyalin paket tersebut untuk dianalisa kemudian oleh hacker yang bersangkutan. Contoh program *sniffer* misalnya pcapture, sniffit dan tcpdump untuk sistem operasi UNIX, WebXRay untuk sistem operasi Windows, Netmon, EtherPeek, LanWatch, dan sebagainya.

Kelemahan tiap sistem operasi komputer biasanya berbeda-beda dan orang yang mempelajari sistem itu secara mendalam akan mengetahuinya dan dapat ***mengeksploitasi kelemahannya*** (kecuali bila ada yang memberi informasi mengenai kelemahan sistem itu). Sebagai contoh adalah kelemahan atau lubang pada sistem yang disebut default username dan password yang sudah diprogram ke dalam beberapa sistem sejak di pabrik. Selain default, kesalahan pada program juga dapat dieksploitasi oleh para penyusup. Program-program baru yang versi awal maupun versi terbarunya

seringkali memiliki bug yang dapat membuat program tersebut mengalami crash dan membuang pemakainya ke sistem operasi. Program lapis luar (menjalankan servis untuk umum) yang bermasalah dan memiliki banyak perintah pengaksesan ke bagian dalam suatu jaringan dapat macet dan melemparkan seseorang pemakai ke dalam jaringan bila program tersebut kebetulan mengalami *crash*. Memori (*stack buffer*) sering menjadi titik lemah (dan menjadi sasaran utama hacker) dalam sistem-sistem demikian. Buffer overflow, misalnya pada server POP (Post Office Protocol) dengan *qpopper* dari *Qualcomm* bisa digunakan langsung untuk mengakses direktori *root*. Pada beberapa perangkat lunak lainnya, biasanya para hacker menciptakan kondisi *buffer overflow* untuk mendapatkan sebuah shell (sebagai hasil proses anak/*child person*) dalam sistem proteksi yang bisa digunakan untuk hacking lebih jauh.

Selain kesalahan pada programnya sendiri, seorang hacker bisa juga mencari kelemahan akibat kesalahan konfigurasi program. Misalnya pada anonymous FTP, yang bila tidak dikonfigurasi dengan benar, bisa dimanfaatkan untuk mengambil file-file penting. Hal yang mirip adalah pada tftp (Trivial File Transfer Protocol), daemon yang dapat menerima perintah transfer file tanpa adanya proteksi password. Contoh yang lebih tua lagi adalah eksploit PFH, yang dulu sering digunakan untuk menghack website.

Cara lain yang cukup umum adalah dengan memanfaatkan setiap CGI (Common Gateway Interface). CGI adalah antarmuka yang memungkinkan komunikasi antar program klien dan server. Script CGI sebenarnya sering digunakan untuk pembuatan efek-efek pada webpage, namun dalam

kaitannya dengan keamanan, sebuah script CGI juga memungkinkan akses file, pencitpaan sehll, maupun pengubahan file secara ilegal. Eksploitasi CGI ini sebenarnya bukan merupakan kesalahan pada bahasa penulisan scriptnya, tetapi merupakan teknik pemrograman yang cerdik (biasanya dengan manipulasi validasi input).

Selain memori dan penggunaan script, ada kalanya hacker menemukan cara untuk mengeksploitasi kelemahan yang muncul dari feature baru suatu, misalnya pada server berbasis Win32. Win32 mendukung dua macam penamaan file, yaitu penamaan file yang panjang dan penamaan file yang pendek yang berguna untuk menjaga kompatibilitas dengan sistem operasi lama. Dalam kasus ini kadang-kadang seorang administrator hanya memprotek file berdasarkan nama pendeknya. Bila hal itu terjadi, hacker bisa mengakali proteksi tersebut dengan mengakses file itu menggunakan nama panjangnya.

Fasilitas *file sharing* (terutama pada Windows NT) juga dapat dieksploitasi kelemahannya. Fasilitas ini bila dikonfigurasi kurang bagus dan memungkinkan sembarang orang untuk mengakses data-data dalam komputer dengan mudah.

Dengan pengalaman, pengetahuan teknis dan pemahaman terhadap jaringan komputer, penyerang meningkatkan eksploitasi terhadap interkoneksi jaringan. Mereka mulai mengalihkan sasaran ke infrastruktur Internet, menyerang suatu area di mana banyak orang dan sistem bergantung padanya. Ancaman serangan terhadap infrastruktur lebih besar karena manajer dan administrator jaringan biasanya hanya berfikir untuk melindungi sistem dan

suatu bagian dari infrastruktur daripada melindungi infrastrukture itu sendiri secara keseluruhan.

Trashing adalah metode untuk mengumpulkan informasi (password) dengan cara membongkar kertas-kertas atau dokumen buangan dari instansi atau perusahaan sasaran. Meskipun cara ini nampak kuno, tetapi cara ini kadang-kadang masih berhasil. Salah satu kasus yang tercatat adalah kasus hacker "Control-C" anggota *Legion of Doom* yang diburu Michigan Bell hingga akhirnya tertangkap pada 1987. Namun nasibnya tidak jelek karena ia sendiri mendapatkan pekerjaan di bidang keamanan komputer di Michigan Bell, sementara wajahnya menghiasa poster-poster internal Michigan Bell (bahkan ia menandatanganinya) dengan pesan peringatan pada karyawan untuk selalu menghancurkan sampah-sampah kertas mereka.

c. Menjelajahi sistem komputer (dan mencari akses yang lebih tinggi)

Setelah seorang hacker berada dalam sebuah sistem, ia kemungkinan akan berkeliling, melihat-lihat isi dari sistem yang baru saja dimasukinya dan mencoba perintah untuk mengetahui fungsinya. Salah satu perintah yang paling sering digunakan dalam sistem UNIX adalah perintah *ls*. Perintah ini serupa dengan perintah dir pada DOS, yang gunanya untuk melihat isi direktori. Perintah lain yang banyak digunakan adalah perintah man, yang digunakan untuk menampilkan *manual online* dari suatu perintah. Sintaksnya adalah man (nama perintah).

Setelah beberapa lama berputar-putar dalam sebuah sistem, mungkin seorang hacker akan melihat bahwa aksesnya amat terbatas, sebatas akses yang dimiliki orang yang *account*nya digunakan. Ia pasti akan berusaha mencari

akese tertinggi (*superuser*) yang memungkinkan ia melakukan apa saja di dalam sistem yang ia masuki. Pencapaian akses tertinggi ditandai dengan diijinkannya hacker tersebut untuk mengakses direktori akar/*root* pada sistem tersebut. Pada UNIX ditunjukkan dengan *prompt #*, dan ini tidak akan didapat dengan mudah kecuali pada komputer milik sendiri atau sistem yang administratornya kurang sadar keamanan.

Cara lain untuk mencari hak akses yang lebih tinggi adalah dengan menggunakan apa yang disebut *trojan horse* atau disingkat *trojan*. *Trojan* sesuai legenda Kuda Troya adalah suatu program yang berguna, namun telah disusupi kode atau perintah untuk menjalankan proses yang ilegal. *Trojan Horse* menurut dokumen RFC 1244 (Site Security Handbook) adalah *A trojan horse program can be a program that does something useful, or merely something interesting. It always does something unexpected. Like steal passwords of copy files without your knowledge.*

Trojan horse adalah suatu program yang mempunyai fungsi yang sepintas terlihat bagus, menarik dan berguna yang menyebabkan orang ingin mendownload dan menjalankannya padahal program itu menghasilkan efek yang kemungkinan besar tidak diinginkan oleh penggunanya. Program ini dapat mencuri password atau mengkopi file tanpa diketahui dan disaradri. Bahaya dari program trojan adalah bahwa yang menjalankan program ini akan mempunyai *user level* yang sama dengan lingkungan yang mengaktifkannya (administrator sistem).

Seorang pengguna yang menjalankan program ini mempunyai akese *read, write* dan *execute* (*root privileged*) maka program yang dijalankannya akan

mempunyai kemampuan akses yang sama (*root privileged*) seperti menghapus file, mengirimkan kepada penyusup tentang semua file yang dibacanya, mengubah file apa saja, menginstal program lain dengan *privileges user* seperti program yang menyediakan *unauthorized network acces*, menginstal virus dan program trojan lain.

Hal ini berarti *user* yang menginstal mempunyai *administrative access* ke operating system, sehingga trojan horse bisa berbuat apa saja sebagaimana dilakukan oleh administrator system. Sistem UNIX dengan *root account*, Microsoft Window NT dengan *administrator account* atau pemakai perseorangan yang mempunyai *administrative access* ke sistem operasi tunggal (Win 95 atau MacOS) harus berhati-hati atas meningkatnya akibat dari trojan horse.

Trojan diciptakan dengan tujuan yang berbeda-beda, namun dalam konteks internet security dan privacy, trojan bertujuan untuk melakukan kegiatan mata-mata, yaitu mencari dan mendapatkan informasi vital tentang sistem operasi yang dipakai di suatu kantor atau perusahaan (*privileged root*) atau berkompromi dengan sistem, menyembunyikan beberap fungsi yang salah satu fungsinya membuka rahasia sistem. Jadi trojan horse bisa melakukan tugas intelijen atau menyabotase. Trojan memerlukan campur tangan manusia untuk menginstalnya.

Trojan digolongkan sebagai bahaya tingkat tinggi karena begitu sulitnya dideteksi. Dalam banyak kasus, trojan dapat dijumpai dalam bentuk binaries, sehingga sukar dibaca dan dipahami oleh bahasa manusia. Trojan adalah

tipe serangan sempurna dan fatal buat *administrator system* yang hanya mempunyai sedikit kemampuan *security*.

Cara lain adalah dengan *decoy*. *Decoy* adalah program tersendiri yang dibuat menyerupai program tampilan login. Decoy menipu pemakai untuk memasukkan nama dan passwordnya ke dalam layar login tersebut. Setelah pemakai memasukkan nama dan passwordnya, decoy akan menyimpan kombinasi tersebut ke dalam sebuah file, menampilkan pesan kesalahan yang memaksa pemakai merestart komputernya, atau keluar dan mengulang login, dan kala pemakai mengulang login, decoy akan mengembalikan pemakai ke sesi login yang sebenarnya.

Cara lain yang lebih sederhana adalah *shoulder surfing*. *Shoulder surfing* ini berarti diam-diam memperhatikan apa yang diketikkan orang lain di komputernya. Tidak perlu teknik tinggi, tetapi agak susah terutama kalau dicoba pada orang yang mahir mengetik 10 jari.

d. Membuat *backdoor* dan menghilangkan jejak

Seorang hacker yang ahli akan berusaha agar aksi dan keberadaannya tidak diketahui oleh pemilik sistem yang dimasukinya, sebab jika ketahuan urusannya akan panjang apalagi jika tertangkap, ujungnya pasti tidak enak. Berkaitan dengan waktu pengguna, cara untuk memperkecil kemungkinan terdeteksi adalah dengan melakukan aktivitasnya di saat sistem yang akan dimasukinya tidak atau kurang diawasi, misalnya pada waktu subuh atau akhir minggu. Berkaitan dengan teknik, salah satu cara yang paling umum adalah mengedit file-file log (catatan aktivitas) pada sistem yang dimasukinya dan menghilangkan semua entry yang berkaitan dengan dirinya.

Aktivitas yang berlangsung selama hacking misalnya saja aktivitas *scanning*, bisa disamarkan dengan memasang kuda troyan ke program-program yang biasa digunakan untuk mengawasi jaringan, misalnya netstat.

Cara lain untuk menyamarkan identitias saat beraksi adalah dengan melakukan *bouncing*. *Bouncing* adalah memanfaatkan suatu sistem sebagai basis operasi untuk memasuki sistem lain. Dalam praktek bouncing ini, jejak-jejak akan mengarah ke komputer yang dijadikan basis operasi dan bukan ke lokasi hacker sebenarnya. *Bouncing* dapat dilakukan melalui FTP, mesin proxy server, wingate atau host lain (dengan memanfaatkan telnet atau rsh). Selain melalui internet, *bouncing* juga bisa dilakukan melalui manipulasi hubungan telepon. Bouncing seperti ini biasanya sukar sekali dilacak, tetapi tingkat kesulitannya juga tinggi. Selain bermanfaat untuk menyulitkan pelacakan, bouncing juga bermanfaat untuk melewati berbagai program proteksi.

Selain berfikir untuk menghilangkan jejak, hacker mungkin juga berfikir untuk kembali ke sistem tersebut pada suatu saat sehingga ia akan membuat *backdoor* (pintu belakang). *Backdoor* pada prinsipnya adalah jalan tembus yang dibuat hacker setelah masuk yang berguna untuk kembali tanpa perlu melalui sistem proteksi lagi. Contoh pemasangan *backdoor* adalah modifikasi file *hosts.equiv* dan *.rhosts* (pada sistem UNIX). Modifikasi pada file-file tersebut memungkinkan komputer host hacker diberi status *trusted* oleh sistem sasaran, hingga pengaksesan dari komputer hacker tidak akan disaring. *Backdoor* juga bisa dibuat dengan menambahkan *account-account* baru pada file daftar password (/etc/passwd pada UNIX standar). Alternatif

dari penambahan *account* ini adalah pembuatan daftar password palsu yang akan ditukar tempatnya dengan file password asli pada waktu-waktu tertentu (dengan bantuan cron - fasilitas administrator waktu pada UNIX).

Selain cara-cara itu, penyalinan *SUID shell* ke direktori yang mudah diakses (misalnya /tmp) juga sering digunakan. Untuk mencegah kecurigaan, nama shell ini akan diubah, misalnya dari /bin/csh, disalin menjadi /tmp/.data01.

Satu lagi cara pembuatan *backdoor* yang umum adalah dengan mengubah konfigurasi servis. Konfigurasi tidak begitu sering diperiksa (berbeda dengan daftar password dan log), sehingga kemungkinan terdeteksi lebih kecil. File-file yang dimodifikasi misalnya /etc/inetd. Modifikasi ini biasanya dilakukan dengan cara mengganti daemon dari servis yang jarang digunakan dengan suatu proses yang akan memberikan shell bagi hacker (terutama akses ke root).

4. Masalah Keamanan Sistem Informasi Berbasis Internet

Permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini menempati kedudukan yang sangat penting, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalu dimutakhirnya sehingga informasi yang diberikan tidak ketinggalan jaman. Di samping itu menjaga keamanan sistem informasi yang dijual itu sama pentingnya dengan menjaga kemutakhiran informasi. Keamanan sistem informasi berbasis internet juga

selalu harus dimutakhirkan untuk mencegah serangan atau perusakan yang dilakukan oleh cracker maupun vandal komputer.

Peralatan dalam pelayanan informasi adalah komputer (hardware dan software), jaringan lokal (LAN) maupun wide area network dan sistem operasi yang dipakai untuk memberikan pelayanan itu. Dengan demikian menjaga keamanan sistem informasi berbasis internet berarti menjaga keamanan dari bekerjanya *tool* yang dipakai itu. Meskipun masalah keamanan sistem informasi menempati kedudukan yang penting, tetapi perhatian para pemilik dan pengelola sistem informasi masih kurang, bahkan menempati kedudukan kedua atau berikutnya dalam daftar-daftar berbagai hal yang dianggap penting dalam pengelolaan sistem informasi berbasis internet.

Ada beberapa hal yang harus dilindungi dalam sebuah sistem jaringan informasi global berbasis internet (cyberspace), yaitu:[34]

a. Isi/substansi data dan/atau informasi yang merupakan input dan output dari penyelenggara sistem informasi dan disampaikan kepada publik atau disebut juga dengan *content*. Dalam hal penyimpanan data dan/atau informasi tersebut akan disimpan dalam bentuk databases dan dikomunikasikan dalam bentuk data messages;
b. Sistem pengolahan informasi (*Computing and/or information system*) yang merupakan jaringan sistem informasi (*computer network*) organisasional yang efisien, efektif dan legal. Dalam hal suatu sistem informasi merupakan

---

[34] Danrivanto Budjijanto, *Aspek-aspek Hukum Dalam Perniagaan Secara Elektronik (E-Commerce)*, Makalah pada Seminar Nasional Aspek Hukum Transaksi Perdagangan via Internet di Indonesia (E-Commerce) di selenggarakan FH UNPAD, Bandung, 22 Juli 2000, hal. 11. Lihat juga Edmon Makarim, *Telematics Law, Cyberlaw, Media, Communication & Information Technologies*, Makalah pada Seminar tentang Cyber Law, diselenggarkan Yayasan Cipta Bangsa di Bandung, 29 Juli 2000, hal. 4

perwujudan penerapan perkembangan teknologi informasi ke dalam suatu bentuk organisasional/organisasi perusahaan (bisnis);

c. Sistem komunikasi (*communication*) merupakan perwujudan dari sistem keterhubungan (*interconnection*) dan sistem pengoperasioan global (*inter-operational*) antar sistem informasi/jaringan komputer (*computer* network) maupun penyelenggaraan jasa dan/atau jaringan telekomunikasi; dan

d. Masyarakat (*Community*) yang merupakan perangkat intelektual (*brainware*) baik dalamkedudukannya sebagai pelaku usaha, profesional penunjang maupun pengguna.

Menjaga keempat aspek itu merupakan bagian dari *policy* keamanan sistem informasi. Keamanan sistem informasi berbasis internet merupakan suatu keharusan yang harus diperhatikan karena jaringan komputer internet yang sifatnya publik dan global pada dasarnya tidak aman. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar informasi yang berharga itu dapat terlindungi secara efektif. Untuk mencapai semua itu, jaringan komputer harus dianalisa untuk mengetahui apa yang harus dan untuk apa diamankan, serta seberapa besar nilainya.

Keamanan komputer (*computer security*) melingkupi empat aspek, yaitu *privacy, integrity, authentication* dan *availability*. Selain keempat aspek itu masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce* yaitu *access control* dan *non-repudiation*.[35] Aspek utama dari ***privacy*** atau ***condifentiality*** adalah usaha untuk menjada informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data-data yang

---

[35] Simon Garfingkel sebagaimana dikutip oleh Budi Rahardjo, *op.cit.* hal. 11-14. Penjelasan lebih lanjut mengenai aspek-aspek ini dapat dibaca pada Budi Rahardjo, *ibid.*

sifatnya privat, sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator, sedangkan contoh *confidentiality* information adalah data-data yang sifatnya pribadi dan merupakan data-data yang diproteksi penggunaan dan penyebarannya. Serangan terhadap aspek privacy ini misalnya adalah usaha untuk melakukan penyadapan (*sniffing*). Usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *condifentiality* adalah dengan menggunakan teknologi *kriptografi* (enkripsi dan dekripsi).

Dalam lingkup *cyberlaw*, yang termasuk *privacy* ada 4 (empat) kategori, yaitu:[36]

a. protection from intrusion;
b. protection from the public disclosure of embarrassing private facts;
c. protection from publicity that places the individual in a false light, and
d. protection from the use of a person's name or likeness.

Hukum biasanya merefleksikan minimum perilaku yang dapat diterima. Meski demikian ada aspek universal dari privacy yang terbentuk dari bagian kehidupan sosial yang integral. Setiap kebudayaan mengakui beberapa bentuk dari privacy, yang diikuti untuk menunjukkan rasa hormat pada orang lain (*immunity from intrusion*) dan pengertian pada diri sendiri (*according a sphere of autonomy*). Ada yang berpendapat bahwa privacy harus dilindungi dan

---

36 Ann K. Moceyunas, *On-line Privacy: the Push and Pull of Self-Regulation and Law*, Net Law News, Oct-Nov-Dec 1999.

ditempatkan tersembunyi pada koleksi data, tetapi ada juga yang berpendapat perlu adanya masyarakat yang transparan (transparent society) di mana akan ada terbuka keseimbangan di antara kekuatan individu dan kekuatan institusi. *The United State Federal Trade Commision* dalam sebuah studinya dari tahun 1995-1998 menentukan bahwa Asosiasi Industri Amerika Serikat menentukan lima prinsip pokok dari koleksi data individual yang perlu dilindungi, yaitu *notice, choice, access, security and enforcement mechanism*.[37]

Aspek ***integrity*** menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. *Virus, trojan horse* atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi pada aspek ini. Sebuah e-mail dapat saja ditangkap (*intercept*) di tengah jalan, diubah isinya (*altered, tampered, modified*), kemudian diteruskan ke alamat yang dituju. Dengan kata lain integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya dapat mengatasi masalah ini.

Aspek ***authentication*** berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Masalah pertama membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan *digital signature*. *Watermarking* juga dapat digunakan untuk menjaga *intelectual property*, yaitu dengan menandai dokumen atau hasil karya dengan tanda tangan pembuat. Masalah kedua biasanya berhubungan dengan *access control*, yaitu berkaitan dengan pembatasan orang yang dapat mengakses

---

[37] Bandingkan dengan persyaratan privacy yang ditentukan dalam The Children's Online Privacy Protection Act 1998 yang menentukan ada lima prinsip, yaitu *notice, consent, disclosure, collection, and security of personally identifiable data. Ibid.*

informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan *password, biometric* (ciri-ciri khas orang) dan sejenisnya. Penggunaan teknologi *smart cord*, saat in kelihatannya dapat meningkatkan kemanan aspek ini. Secara umum proteksi authentication dapat menggunakan *digital certificates.*

Aspek ***availability*** atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadaan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan *denial of service attack* (DoS attack), di mana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash.* Contoh lain adalah adanya *mailbomb*, di mana seorang pemakai dikirimi e-mail bertubi-tubi (katakanlah ribuah e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka emailnya atau kesulitan mengakses e-mailnya. Serangan terhadap *availability* dalam bentuk DoS attack merupakan yang terpopuler pada saat ini.

Access control berhubungan dengan cara pengaturan akses pada informasi. Hal ini biasanya berhubungan dengan masalah *authentication* dan juga *privacy. Access control* seringkali dilakukan dengan menggunakan kombinasi *userid/password* atau dengan menggunakan mekanisme lain. Asoek ***non-repudiation*** ini menjaga agar seseorang tidak dapat meyangkal telah melakukan sebuah transaksi. Contohnya jika seseorang mengirimkan em-amil untuk memesan barang, tidak dapat menyangkal bahwa dia telah mengirimkan e-mail tersebut. Aspek ini sangat penting dalam hal *electronic commerce.*

Penggunaan *digital signature, certificates* dan teknologi *kriptografi* secara umum dapat menjaga aspek ini, akan tetapi masih harus didukung oleh hukum, sehingga statusnya dari *digital signature* itu jelas legal.

Meskipun sebuah sistem informasi sudah dirancang memiliki perangkat pengamanan yang baik, dalam operasi masalah ini harus selalu dimonitor karena resiko, ancaman dan *vulnerabilities* setiap saat akan mengancam dan menyerang apabila pengelola sistem atau administrator lengah. Menjaga kemutakhiran keamanan sistem informasi ini penting karena beberapa hal, yaitu:[38]

1) Ditemukannya lubang keamanan (*security hole*) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks, sehingga tidak mungkin untuk diuji seratus persen, kadang-kadang ada lubang keamanan yang ditumbulkan oleh kecerobohan implementasi.
2) Kesalahan konfigurasi. Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan.
3) Penambahan perangkat baru (hardware dan/atau software) yang menyebabkan menurunnya tingkat *security* atau berubahnya metode untuk mengoperasikan sistem sehingga operator atau administrator sistem harus belajar lagi.

Lubang keamanan selain dapat ditemukan sebagai akibat kompleksnya suatu sistem (yang menyebabkan tidak bisa diuji satu persatu), juga dapat dibuat atau ditembus oleh para kriminal atau cracker dengan keahlian yang dimilikinya. Para kriminal itu selain mempunyai keahlian membongkar sistem keamanan juga dapat memperoleh informasi mengenai kelemahan sistem operasi dari internet

---

38 Budi Rahardjo, *op.cit.* hal. 39-40

yang memudahkan kerja mereka. Menurut **David Icove**, berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:[39]

1) Keamanan yang bersifat fisik (*physical security*), termasuk akses orang ke gedung, peralatan dan media yang digunakan. Beberapa *cracker* mengatakan bahwa mereka sering pergi ke tempat sampah untuk mencari berkas-berkas yang mungkin memiliki informasi tentang keamanan (seperti coretan *password* ataupun *wiretapping*, yaitu hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan).
2) Keamanan yang berhubungan dengan orang (*personal*), termasuk identifikasi dan profil resiko dari orang yang mempunyai akses (pekerja). Seringkali kelemahan keamanan sistem informasi bergantung kepada manusia (pemakai dan pengelola). Teknik yang biasa digunakan dalam kategori ini adalah *social engineering*.
3) Keamanan dari data dan media serta teknik komunikasi (*communications*), yang termasuk dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang virus atau *trojan horse* sehingga dapat mengumpulkan informasi (seperti password) yang semestinya tidak berhak diakses.
4) Keamanan dalam operasi, termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga prosedur setelah serangan.

Lubang keamanan dapat terjadi karena beberapa hal, yaitu salah desain (*design flaw*), salah implementasi, salah konfigurasi dan salah penggunaan.[40] Lubang keamanan yang disebabkan oleh ***salah disain*** pada umumnya jarang terjadi, tetapi apabila terjadi sulit diperbaiki. Meskipun suatu sistem operasi

---

[39] David Icove sebagaimana dikutip oleh Budi Rahardjo, *Ibid*, hal. 9-10
[40] Budi Rahardjo, *Ibid*. hal. 40-42

diimplementasikan dengan baik apabila terjadi salah desain maka kelemahan dari sistem akan tetap ada. Contoh lubang keamanan yang dapat dikategorikan ke dalam kesalahan desain adalah desain urutan nomor (*sequence numbering*) dari paket TCP/IP. Kesalahan ini dapat dieksploitasi sehingga timbul masalah yang dikenal dengan nama *IP spoofing*, yaitu sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah mengamati urutan paket dari host yang hendak di serang.

Lubang keamanan yang disebabkan oleh ***kesalahan implementasi*** sering terjadi. Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean, akibatnya cek atau testing yang harus dilakukan menjadi tidak dilakukan. Sebagai contoh seingkali batas (*bound*) dari sebuah *array* tidak dicek sehingga terjadi yang disebut *out-of-bound array* atau *buffer overflow* yang dapat dieksploitasi. Lubang keamanan yang terjadi karena masalah ini sudah sangat banyak, dan yang mengherankan terus terjadi, seolah-olah para programer tidak belajar dari pengalaman.

Meskipun program sudah diimplementasikan dengan baik, masih dapat terjadi lubang keamanan karena ***salah konfigurasi***, misalnya berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi *writeable*. Apabila berkas tersebut berkas yang penting, seperti berkas yang digunakan untuk menyimpan password, maka efeknya menjadi terbuka lubang keamanan. Contoh lain misalnya ada program yang secara tidak sengaja diset menjadi *setuid root*, sehingga ketika dijalankan pemakai memiliki akses seperti *super user* (*root*) yang dapat melakukan apa saja.

Salah penggunaan program dapat juga mengakibatkan terjadinya lubang keamanan. Kesalahan menggunakan program yang dijalankan dengan menggunakan *account root* (*super user*) dapat berakibat fatal. Kesalahan menggunakan program ini berakibat seluruh berkas yang ada pada sistem itu menjadi hilang dan akibat lebih jauh adalah *Denial of Service* (DoS). Apabila sistem itu digunakan secara bersama-sama, maka akibatnya lebih fatal lagi.

Security attack atau serangan terhadap keamanan sistem informasi dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Menurut **W. Stallings**, ada beberapa kemungkinan serangan (*attack*), yaitu:[41]

1) *Interruption*: perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah *denial of service attack*.
2) *Interception*: pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*Wiretapping*)
3) *Modification*: pihak yang tidak berwenang selain berhasil mengakses, dapat juga mengubah (*tamper*) aset. Contoh dari serangan ini adalah mengubah isi dari website dengan pesan-pesan yang merugikan pemilik website
4) *Fabrication*: pihak yang tidak berwenang menyisipkan obyek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Onno W. Purbo dan **Tonny Wiharjito** menyebut serangan (*attack*) itu dengan istilah insiden keamanan jaringan komputer. Insiden keamanan jaringan

---

[41] William Stallings, *Network and Internetwork Security*, Prentice Hall, 1995, hal. 28.

komputer merupakan aktivitas yang berkaitan dengan jaringan komputer yang memberikan implikasi terhadap keamanan. Secara garis besar, insiden keamanan jaringan komputer berupa *probe, scan, account compromize, root compriomize, packet sniffer, denial of service, exploitation of trust, malicious code* dan *Internet infrastructure attacks.*[42]

Probe merupakan usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem atau untuk menemukan informasi tentang sistem tersebut, misalnya usaha untuk login ke dalam sebuah *account* yang tidak digunakan. Kadang-kadang *probe* diikuti dengan aktivitas lain yang sifatnya berbahaya terhadap keamanan jaringan komputer atau hanya untuk memuaskan rasa penasaran si pelaku. Kegiatan si penyusup setelah probe ini dinamakan ***account compromise***. Jika si penyusup itu berhasil masuk secara ilegal dan memperoleh *privilege* sebagai administrator sistem (*superuser*) maka ia mempunyai kemampuan melakukan apa saja pada sistem yang menjadi korban termasuk menjalankan program, mengubah kinerja sistem dan menyembunyikan jejak penyusupan. Kegiatan yang mirip dengan *account* compromise ini disebut ***root compromise***.

Scan adalah kegiatan *probe* dalam jumlah yang lebih besar dengan menggunakan *tool* secara otomatis. *Tool* tersebut secara otomatis mendeteksi kelemahan pada host lokal maupun host remote. Sebuah *scanner* sebenarnya adalah *scanner* untuk prot TCP/IP yaitu sebuah program yang menyerang port TCP/IP dan servis-servisnya (telnet, ftp, http dan sebagainya) dan mencatat respon dari komputer target. *Tool-tool* untuk scanning yang umum digunakan

---

42 Penjelasan lebih lengkap dan jelas dapat dibaca pada Onno W. Purbo dan Tony Wiharjito, *op.cit*, hal. 9-20

antara lain *SATAN, JAKAL, IdentTCPScan, CONNECT, XSCAN, FSPScan*, dan lain-lain.

Packet sniffer adalah sebuah device, baik perangkat lunak maupun perangkat keras yang digunakan untuk memperoleh informasi yang melewati jaringan komputer yang menggunakan protokol apa saja (Ethernet, TCP/IP, IPX dan sebagainya). Sebuah *sniffer* dapat berupa dan biasanya merupakan kombinasi perangkat lunak dan perangkat keras. Kedudukan *sniffer* pada keamanan jaringan komputer sangat penting karena *sniffer* dapat menyadap password, dapat menyadap informasi rahasia dan dapat digunakan untuk membongkar keamanan di dalam suatu jaringan.

Denial of service atau penolakan terhadap servis dapat terjadi karena beberapa hal, tetapi sulit untuk memperkirakan penyebab penolakan itu. Berikut ini adalh beberapa contoh penyebab terjadinya penolakan terhadap servis:

1) Kemungkinan jaringan menjadi tidak berfungsi karena kebanjiran trafik
2) Kemungkinan jaringan dipartisi dengan cara membuat komponen jaringan (misalnya router) yang menjadi penghubung jaringan menjadi tidak berfungsi
3) Kemungkinan ada virus yang menyebar dan menyebabkan sistem komputer menjadi lambat atau bahkan lumpuh
4) Kemungkinan device yang melindungi jaringan dirusakkan.

Si penyusup atau penyerang dapat saja masuk secara ilegal ke dalam suatu sistem dan mengeksploitasi kelemahan yang ada. Ini dapat terjadi apabila si penyusup berhasil membuat identitas palsu yang menyerupai dengan identitas dari orang yang diberi kepercayaan untuk melakukan akses legal ke dalam suatu

sistem. Dengan kata lain, si penyusup ***mengeksploitasi kepercayaan*** dari orang yang identitasnya berhasil disamarkan itu. Kegiatan ini seperti *probe* dan jika berhasil masuk dan melihat-lihat sistem maka seperti *account compromise* bahkan dapat seperti *root compromise*.

Malicious code merupakan program yang apabila dieksekusi akan menyebabkan sesuatu yang tidak diinginkan terjadi. Termasuk dalam malicious code ini adalah *trojan horse, virus* dan *worm*. *Trojan horse* dan *virus* biasanya disusupkan ke dalam suatu file atau program sedangkan *worm* adalah program yang dapat menduplikasikan diri dan menyebar tanpa intervensi manusia setelah program tersebut dijalankan. Virus juga dapat menduplikasikan diri, tetapi perlu intervensi dari user komputer. *Malicious code* ini dapat menyebabkan kerusakan atau kehilangan data yang serius, penolakan terhadap servis dan jenis-jenis insiden lain.

Insiden ***serangan terhadap infrastruktur Internet*** jarang terjadi tetapi merupakan insiden yang serius. Serangan ini mencakup komponen-komponen pokok dari infrastruktur Internet, tidak hanya mencakup sistem yang khusus dari Internet. Contohnya adalah server network, name server, network access provider. Penyebarannya secara luas sebuah serangan yang diatur secara otomatis juga dapat mengancam infrastruktur Internet yang menyebabkan sebagian besar dari Internet tidak dapat berfungsi sebagaimana mestinya.

Untuk menjaga agar keamanan jaringan komputer tetap baik, semua data dan file yang bersifat rahasia tetap terlindungi, maka perencanaan kebijakan (*policy*) pengamanan jaringan komputer perlu dilakukan. Perencanaan kebijakan pengamanan jaringan komputer ini dilakukan untuk mengamankan aset dan

sumber daya yang ada dan tertanam di jaringan komputer itu. Ada beberapa hal yang perlu diperhatikan dalam perencanaan kebijakan keamanan jaringan komputer, yaitu:[43]

1) Resiko

Resiko (*risk*) merupakan suatu kemungkinan di mana penyusup berhasil mengakses komputer di dalam jaringan yang dilindungi. Apa yang dilakukan oleh si penyusup (mengeksekusi file, merusak data dan sebagainya) akan menimbulkan kerugian. Si penyusup dapat saja memperoleh dan menggunakan suatu *account* dengan cara menyamar dan akibat lebih jauh adalah seluruh jaringan komputer menjadi tidak aman.

Dalam menghadapi resiko ini, **Lawrie Brown** menyarankan menggunakan *Risk Management Model* untuk menghadapi ancaman (*managing threats*). Ada tiga model komponen yang memerikan kontribusi kepada *Risk*, yaitu *Asset, Vulnerabilites* dan *Threats*. *Asset* ini meliputi hardware, software, dokumentasi, data, komunikasi, lingkungan dan manusia. *Threats* meliputi pemakai (*users*), teroris, kecelakaan (*accidents*), crackers, penjahat/kriminal, nasib (*acts of God*) dan intel luar negeri (*foreign intelligence*). *Vulnerabilities* meliputi *software bugs, hardware bugs*, radiasi (dari layar, transmisi), *tapping, crosstalk, unauthorized users*, cetakan, *hardcopy* atau *print out*, keteledoran (*oversight*), cracker via telepon dan *storage media*.

Untuk menanggulangi resiko tersebut dilakukan apa yang disebut *countermeasures* yang dapat berupa usaha mengurangi *threat,*

---

[43] Onno W. Purbo & Tony Wiharjito, loc.cit., hal. 2-4. Lihat juga Budi Rahardjo, op.cit, hal. 2-4

vulnerabilities, *impact*, mendeteksi kejadian yang tidak bersahabat (*hostile event*), dan kembali (*recover*) dari kejadian

2) Ancaman

Ancaman bisa datang dari siapa saja yang mempunyai keinginan untuk memperoleh akses ilegal ke dalam suatu jaringan komputer. Untuk itu diperlukan tindakan berupa penentuan siapa saja yang boleh mempunyai akses legal ke dalam sistem itu. Penyusup mempunyai beberapa tujuan yang ingin dicapai dengan penyusupannya itu. Pengetahuan mengenai tujuan tindakan penyusup ini sangat berguna dalam merencanakan sistem keamanan komputer. Beberapa tujuan para penyusup itu antara lain:

a) Pada dasarnya hanya ingin tahu sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut dengan *The Curious*

b) Membuat sistem jaringan komputer menjadi *down*, atau mengubah tampilan situs web, atau hanya ingin membuat organisasi pemilik jaringan komputer sasaran harus mengeluarkan uang dan waktu untuk memulihkan jaringan komputernya. Penyusup yang mempunyai tujuan seperti ini sering disebut dengan *The Malicious*.

c) Berusaha untuk menggunakan sumber daya di dalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup jenis ini sering disebut dengan *The High-Profile Intruder*

d) Ingin tahu data apa yang ada di dalam jaringan komputer sasaran untuk selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup jenis ini sering disebut dengan *The Competition*.

3) Kelemahan

Kelemahan pada suatu jaringan komputer menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain dan kemungkinan bagi seseorang untuk mendapat akses ilegal ke dalamnya. Kelemahan suatu jaringan komputer apabila dieksploitasi oleh penyusup dapat menimbulkan kerugian yang tidak sedikit, bukan hanya biaya perbaikan tetapi juga waktu yang diperlukan untuk membuat jaringan itu kembali normal.

Perencanaan kebijakan keamanan situs yang dimaksud meliputi keamanan terhadap seluruh sumber daya yang tertanam dalam jaringan komputer tersebut. Suatu perusahaan dapat memiliki beberapa situs dan situs pada umunya adalah bagian dari organisasi yang mempunyai beberapa komputer dan sumber daya yang terhubung ke dalam suatu jaringan. Sumber daya tersebut misalnya workstation, komputer sebagai host maupun server, device untuk interkoneksi seperti gateway, router, bridge, repeater, terminal server, perangkat lunak aplikasi dan jaringan, kabel jaringan dan informasi di dalam file dan basis data. Policy kemanan yang hendak direncanakan itu harus meliputi keamanan semua sumber daya itu.

5. Konstruksi *Hacking* Sebagai Kejahatan

Perkembangan teknologi informasi telah mengubah hampir semua sisi kehidupan. Pada satu sisi teknologi komputer memberikan keuntungan berupa kesempatan untuk mendapatkan informasi, pekerjaan, berpartisipasi dalam politik dan kehidupan berdemokrasi serta keuntungan lain, akan tetapi pada sisi lain ia akan semakin menggerogoti kehidupan nyata yang telah lama kita geluti

dengan segala peninggalan yang ada. Para *netizen* dapat melihat hal ini sebagai suatu persoalan yang harus dipecahkan sebelum ia bergerak lebih jauh menyelusuri jalan dan lorong-lorong *cyberspace*.

Bagi mereka yang memanfaatkan teknologi informasi ini untuk kegiatan bisnis, pelayanan publik dan media hiburan, membangun situs-situs yang dapat dikunjungi oleh para *netizen*, harus berhati-hati dan membangun sistem keamanan yang handal karena tidak semua *netizen* atau pengakses yang berkunjung ke dunia maya dan menikmati realitas virtual yang ditawarkan adalah orang baik-baik. Seperti halnya dalam kehidupan nyata, di sana juga ada kejahatan yang dampaknya akan dirasakan dalam kehidupan nyata.

Hacking merupakan salah satu kegiatan yang bersifat negatif tersebut. Meskipun pada awalnya *hacking* memiliki tujuan mulia, yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya, tetapi dalam perkembangannya *hacking* digunakan untuk keperluan-keperluan lain yang bersifat merugikan. Hal ini tidak lepas dari penggunaan internet yang semakin meluas sehingga penyalagunaan kemampuan *hacking* juga mengikuti luasnya pemanfaatan internet.

Dari hasil penelitian yang telah dijelaskan pada bagian sebelumnya, maka dapat disimpulkan beberapa tahap *hacking* yang selanjutnya akan digunakan sebagai langkah untuk menentukan tahap-tahap *hacking* yang dapat dikonstruksikan sebagai kejahatan. Tahap-tahap *hacking* seperti yang dimaksud adalah:

a. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran.

a. Menyusup atau mengakses jaringan komputer target sasaran

b. Menjelajahi sistem komputer (dan mencari akses yang lebih tinggi)

c. Membuat *backdoor* dan menghilangkan jejak

Hacker harus memiliki pengetahuan dan kemampuan menguasai serta mengaplikasikan bahasa pemrograman. Pengetahuan dan kemampuan itu dapat diperoleh dengan berbagai cara, di antaranya dengan belajar pada ahlinya atau belajar sendiri secara otodidak. Bahasa pemrograman merupakan bahasa teknis, sehingga orang yang benar-benar tidak mempunyai kemampuan teknis (meskipun hanya kemampuan teknis dasar komputer) akan kesulitan untuk memahani bahasa teknis ini.

Proses belajar menjadi seorang hacker atau cracker dalam perspektif kriminologi terutama dari *teori differential association* ataupun dalam perkembangannya yang disebut *differential social organization* dari **Sutherland**[44] sudah menunjukkan bahwa orang yang belajar itu sedang mempelajari atau belajar menjadi seorang penjahat. Bagi **Sutherland** semua tingkah laku itu dipelajari, tidak terkecuali untuk menjadi penjahat. Jadi dalam perspektif ini untuk menjadi penjahat di *cyberspace* (*cracker*) harus melalui proses pembelajaran.

Seorang hacker dapat meningkatkan kemampuannya hackingnya melalui proses komunikasi dan interaksi dengan orang lain terutama dengan orang-orang yang memiliki pengetahuan *hacking* lebih baik atau bergaul dan masuk dalam

---

[44] Versi pertama dari teori differential association ataupun social disorganization dari Sutherland muncul pada tahun 1939 pada bukunya yang berjudul Principles of Criminology, kemudian versi kedua muncul pada tahun 1947 dengan mengganti pengertian social disorganization dengan differential social organization dengan mengajukan sembilan pernyataan yang intinya adalah "semua tingkah laku itu dipelajari" tidak terkecuali untuk berperilaku sebagai penjahat.

kelompok-kelompok hacker/cracker. Tetapi untuk berkomunikasi atau berinteraksi dengan mereka bukanlah perkara yang mudah, dibutuhkan perjuangan yang cukup berat.

Pengetahuan dan kemampuan menguasai serta mengaplikasikan bahasa pemrograman berupa kemampuan mengetahui kelemahan, kekurangan dan kelebihan serta kemungkinan pengembangan bahasa pemrograman yang dikuasai itu menjadi lebih sempurna (seperti yang dilakukan oleh **Linus Torvalds** dengan Linuxnya). Jika seseorang hanya mengetahui dan menggunakan bahasa pemrograman tanpa memiliki pengetahuan tentang kelemahan sistem operasi, maka orang tersebut hanya dapat disebut sebagai *users* (pengguna) saja dan tidak dapat disebut sebagai programer ataupun hacker.

Dengan melihat pada tahap-tahap dalam *hacking*, kemampuan mengidentifkasi dan memastikan apakah sebuah sistem operasi pada target sasaran dapat di*hack* atau tidak, sangat tergantung pada pengetahuan dan kemampuan menguasai, mengaplikasikan serta mengeksploitasi bahasa pemrograman itu. Meskipun seseorang mengetahui sebuah perusahaan yang menggunakan jaringan komputer dengan sistem operasinya sebagai sarana untuk menunjang pekerjaannya, tetapi dia tidak dapat melakukan hacking apabila bahasa pemrogramam yang dimiliki dan dikuasainya berbeda dengan yang dipakai pada target sasaran.

Setiap sistem operasi mempunyai kelemahan. Kelemahan itu lambat laun akan diketahui oleh para hacker melalui berbagai cara, di antaranya adalah mempelajari sistem operasi tersebut, diskusi dengan sesama hacker melalui *mailing list*, *newsgroup* maupun mengambil informasi dari sebuah situs di

internet yang menyajikan informasi mengenai kelemahan-kelemahan sistem operasi komputer. Kemudahan memperoleh informasi mempermudah seseorang untuk menjadi hacker, cracker ataupun bogus hacker.

Berusaha untuk mengetahui sesuatu bukanlah kejahatan. Mencari dan mengumpulkan informasi mengenai suatu sistem operasi yang digunakan pada sebuah perusahaan atau instansi pemerintah juga bukan merupakan kejahatan karena keingintahuan merupakan sifat yang manusiawi. Informasi adalah bebas, ia bergerak ke mana saja dan hak untuk mendapatkan informasi merupakan hak asasi yang dijamin dengan undang-undang. Pembatasan atau larangan terhadap kebebasan mendapatkan informasi merupakan halangan untuk menumbuhkan daya kreatif dan pengembangan ilmu pengetahuan dan teknologi. Kebebasan informasi dan hak untuk mendapatkannya merupakan prinsip yang dipegang teguh oleh seorang hacker. Dengan demikian mempelajari dan mengumpulkan informasi mengenai sistem operasi komputer yang digunakan oleh target sasaran bukanlah kejahatan.

Mengetahui dan mempunyai informasi mengenai kelemahan sistem operasi tidak dapat dikategorikan sebagai kejahatan. Jika orang dilarang untuk mencari dan mengumpulkan informasi mengenai sebuah sistem operasi, dapat dipastikan sistem operasi itu tidak akan berkembang dan tentunya pengetahuan dan penguasaan teknis komputer yang dimiliki oleh berbagai bangsa di dunia ini akan terbelakang. Pengembangan komputer dan jaringan komputer hanya dapat diberlangsung jika informasi bisa diakses oleh semua orang, khususnya orang yang berminat mempelajari dan mengembangkan bahasa pemrograman beserta sistem operasinya.

Apa yang dikhawatirkan dari orang yang memiliki pengetahuan dan kemampuan menguasai serta mengaplikasikan bahasa pemrograman pada sistem operasi yang tepat adalah maksud jahat yang tersembunyi dari keingintahuan suatu sistem operasi yang dipakai pada target sasaran. Apabila hanya ingin mengetahui sistem operasi yang dipakai saja, tidak apa-apa, karena ini merupakan bagian dari sifat manusia yang ingin serba tahu, akan tetapi apabila pengetahuan yang dimilikinya itu kemudian digunakan untuk melakukan perbuatan jahat, itu yang tidak bisa ditolerir.

Langkah hacker setelah mengetahui sistem operasi apa yang dipakai pada target sasaran adalah menyusup atau mengakses jaringan komputer target sasaran itu. Menyusup atau mengakses jaringan komputer target sasaran ini dilakukan dengan mengeksploitasi kelemahan yang ada pada sistem operasi tersebut, dengan kata lain hacker memasuki situs orang lain tanpa ijin. Hacker dengan kemampuannya dapat masuk dan berjalan-jalan dalam situs orang lain meskipun situs itu telah dilengkapi dengan sistem keamanan. Tantangan bagi hacker adalah membongkar sistem keamanan yang digunakan. Jika langkah ini dapat dilakukan, maka merupakan kebanggaan tersendiri bagi hacker, setidak-tidaknya merupakan modal untuk mendapatkan pengakuan mengenai status dirinya dari sesama hacker.

Jika kita membuka situs sebuah situs, misalnya situs kompas dengan alamat http://www.kompas.com atau situs lainnya, maka akan muncul tampilan surat kabar yang dapat dibaca ataupun di*download*. Dengan teknologi *hypertext mark up language* maka kita dapat mencari informasi mengenai berbagai hal, termasuk terbitan kompas pada hari sebelumnya. Apa yang ditampilkan dalam situs

kompas dapatlah disebut sebagai ruang yang bisa dilihat dan dinikmati oleh pengunjung situs itu. Itu yang dinamakan ruang publik atau ruang untuk pelayanan publik atau disebut juga ruang yang bersifat sosial.

Di samping ruang yang bersifat sosial itu, ada pula ruang yang bersifat privat atau ruang yang hanya bisa dimasuki oleh orang-orang tertentu yang mempunyai kode akses atau nomor pin yang diberikan oleh administrator sistem. Bagaimana tampilan dalam situs itu dibuat, mengubah isi atau mengaktualkan berita-berita yang ditampilkan dan setiap saat dapat berubah serta membuat gambar atau tampilan dalam situs agar selalu menarik, merupakan ruang yang hanya bisa dimasuki oleh orang-orang yang memiliki akses dan kemampuan dalam mendesain tampilan. Orang yang memiliki kemampuan mendesain tampilan situs dalam internet itulah yang disebut dengan nama *Webmaster*.

Ruang privat ini tidak bisa dimasuki oleh sembarang orang. Apabila digambarkan sebuah situs adalah seperti sebuah rumah dengan pekarangannya, maka apa yang bisa dilihat dari luar, itulah yang bisa diberikan oleh pemilik rumah untuk dinikmati oleh orang lain sebagai perwujudan dari fungsi sosial rumah itu. Tetapi apabila orang ingin masuk ke rumah itu (meskipun hanya ingin masuk tanpa maksud lain apapun) maka ia harus mendapatkan ijin dari pemilik rumah, jika tetap nekad untuk masuk maka ia dapat didakwa melanggar privasi orang, apalagi jika diikuti dengan tindakan lain yang bersifat merugikan. Sifat sosial dari sebuah situs adalah apa yang bisa dilihat dan dinikmati dari situs itu, hal-hal lain yang tidak bisa dinikmati berarti masuk dalam ruang privat.

Seorang hacker akan berusaha untuk memasuki ruang privat ini. Meskipun ruang privat ini terlindung dengan sistem keamanan yang berlapis-

lapis, hacker akan tetap berusaha menembusnya. Hacker ingin mengetahui isi dari ruang privat dengan menggunakan bahasa pemrograman yang dikuasainya. Tampilan-tampilan dalam situs internet dibuat dengan menggunakan bahasa pemrograman tertentu, dan hacker dengan penguasaan bahasa pemrograman yang baik dapat merusak tampilan-tampilan itu dan menggantinya dengan tampilan lain yang lebih buruk bahkan mungkin lebih baik.

Memasuki ruang privat dalam sebuah situs internet jelas-jelas dilarang karena akan menyebabkan terganggunya fungsi ruang privat itu apalagi jika diikuti dengan tindakan lebih lanjut yang bersifat destruktif. Mengingat hal tersebut maka langkah kedua dari *hacking* ini sudah dapat dikategorikan sebagai kejahatan.[45] Ruang privat adalah ruang yang bersifat pribadi dan hanya dapat dimasuki hanya oleh orang-orang yang memiliki kode akses tertentu, apabila dimasuki dan informasi yang ada di dalamnya disebarluaskan, maka hal tersebut akan menimbulkan kerugian yang tidak sedikit jumlahnya.

Seorang hacker tidak akan puas apabila hanya melihat-lihat saja seperti halnya pencuri yang tidak akan puas hanya melihat barang-barang yang ada dalam ruang yang dapat dimasukinya. Ia akan menjelajahi ruang-ruang privat yang ada dan mencari ruang utama, pengendali dari semua ruang atau dengan kata lain untuk mencari akses yang lebih tinggi. Jika hanya mengandalkan pada akses yang diperoleh dan menggunakan hak akses ilegal itu untuk menyusup, maka hak akses itu mempunyai kemampuan yang terbatas untuk melihat semua file, sebatas akses yang dimiliki orang yang *account*nya digunakan.

---

[45] Bandingkan dengan ketentuan yang terdapat dalam Pasal 550 dan Pasal 551 KUHP. Dengan melakukan interpretasi terhadap pasal tersebut, maka tahap *hacking* yang pertama ini menurut KUHP dapat dikategorikan sebagai pelanggaran.

Seorang hacker akan berusaha mencari akses tertinggi (*superuser*) yang memungkinkan ia melakukan apa saja di dalam sistem yang ia masuki. Pencapaian akses tertinggi ditandai dengan diijinkannya hacker tersebut untuk mengakses direktori akar atau *root* pada sistem tersebut. Akses tertinggi hanya dimiliki oleh adiministrator sistem dan jika hacker sampai ke tingkat akses tertinggi maka ia dapat berlaku sebagai administrator sistem bahkan dapat menghapuskan semua file-file penting termasuk kode akses yang dimiliki oleh administrator sistem sehingga administrator itu nantinya tidak dapat masuk ke dalam sistem yang dikelola atau dibuat sendiri. Dengan memiliki akses tertinggi itu, seorang hacker "mengkudeta" administrator sistem. Ia dapat bertindak sebagai administrator sistem, dapat melihat-lihat file yang paling rahasia, mengcopy dan memindahkannya ke lain file.

Untuk mendapatkan akses tertinggi ini, seorang hacker dapat menggunakan *trojan horse*. Dengan trojan horse seorang hacker mempunyai *administrative access* ke *operating system*, sehingga *trojan horse* bisa berbuat apa saja sebagaimana dilakukan oleh administrator system. Dalam konteks *internet security* dan *privacy*, *trojan* bertujuan untuk melakukan kegiatan mata-mata, yaitu mencari dan mendapatkan informasi vital tentang sistem operasi yang dipakai di suatu kantor atau perusahaan (*privileged root*) atau berkompromi dengan sistem, menyembunyikan beberap fungsi yang salah satu fungsinya membuka rahasia sistem. Jadi *trojan horse* bisa melakukan tugas intelijen serta dapat pula menyabotase.

Menyusup saja sudah dapat dikategorikan sebagai kejahatan, apalagi sampai menjelajah dan mendapatkan akses tertinggi dari sebuah sistem serta mengambil alih fungsi administrator sistem. Tindakan hacker pada tahap kedua ini tidak dapat ditolerir karena akan mengacaukan sistem, menghambat kerja dan layangan publik yang diberikan target sasaran seperti yang dialami oleh korban-korban hacker. Mereka untuk beberapa saat tidak dapat melakukan layanan publik dan ini merupakan kerugian tersendiri di samping kerugian yang diderita untuk memulihkan kerja sistem komputer.

Seorang pencuri atau perusak bahkan seorang perampok tidak akan tinggal lama-lama di tempat kejadian atau di tempat di mana ia melakukan aksinya sebab akan berbahaya jika ia terus tinggal dan dapat ditangkap oleh pihak yang berwajib. Hal yang sama berlaku untuk seorang hacker yang melakukan aksinya. Ia hanya akan tinggal dalam situs yang berhasil dihack untuk beberapa saat, kecuali jika administrator sistem tidak menyadari situs yang dikelolanya dihack, maka hacker akan menikmati keberadaannya di tempat yang baru.

Jika hacker telah selesai dengan misinya maka ia akan meninggalkan tempat yang telah dijelajahinya. Ia tidak akan begitu saja meninggalkan situs yang berhasil dihack itu, tetapi biasanya ia akan memberikan kenang-kenangan kepada pemilik atau administrator sistem yang situsnya dihack. Kenang-kenangan itu dapat berupa berubahnya tampilan-tampilan situs dengan gambar yang sama sekali lain dari aslinya atau isi situs yang telah diacak-acak atau diganti dengan hal-hal lain yang tidak berkaitan dengan persoalan yang dikelola situs tersebut. Pada umumnya para hacker meninggalkan jejak dengan mengganti tampilan dari situs dengan pesan-pesan yang menunjukkan pemberitahuan bahkan penghinaan terhadap pengelola situs dan jika perlu meninggalkan alamat

situs atau e-mail yang bisa dihubungi (biasanya alamat situs atau e-mail ini tidak benar atau bohong).

Hacker yang meninggalkan jejak seperti itu akan dengan mudah diketahui oleh administrator sistem dengan melihat *log file* (daftar log in dan log out) yang ada pada sistem komputer itu. Dalam *log file* dapat diketahui kapan ia masuk dan kapan ia keluar, serta dapat pula diketahui dari mana asal hacker yang menyusup itu. Bagi hacker meninggalkan jejak seperti itu sangat berbahaya karena keberadaan dan aksinya dapat diketahui meskipun ia melakukan *hacking* tidak dengan komputer pribadinya. Seorang hacker dapat melakukan *hacking* di warung internet dan warung internet yang baik mempunyai *log file* yang dipelihara untuk beberapa waktu lamanya. Jika jejak yang ditinggalkan hacker pada situs yang berhasil dihack menunjuk pada warung internet maka warung internet yang baik itu dapat menunjukkan siapakah sebenarnya hacker itu.

Meninggalkan jejak seperti itu tentu tidak nyaman bagi hacker, sehingga ada kecenderungan dari hacker agar tidak meninggalkan jejak sama sekali, yaitu dengan menghapus semua file log dan file-file lain. Cara ini menyebabkan situs yang dihack tidak mengeluarkan data ketika diakses atau tidak ada tampilannya sama sekali. Cara seperti ini telah memakan beberapa korban (di antaranya adalah LIPI dan Departemen Perindustrian dan Perdagangan) dan jika tidak ada back up-nya, maka kerugian yang timbul akan semakin besar.

Hacker juga memiliki kerinduan, artinya ia mempunyai keinginan untuk kembali lagi ke situs yang berhasil dihack itu. Untuk itu sebelum meninggalkan jejak ia akan membuat backdoor atau pintu belakang yang sewaktu-waktu dapat digunakan untuk masuk kembali. Pembuatan backdoor ini dilakukan ditempat yang memungkinkan administrator tidak dapat menemukannya sebab jika administrator sistem berhasil menemukan maka backdoor ini akan ditutup dan

hacker tidak dapat langsung masuk ke dalam sistem atau dengan kata lain harus mulai dari awal lagi.

Dari penjelasan tersebut dapatlah disimpulkan bahwa *hacking* dilakukan melalui beberapa tahap. Tidak setiap tahap dari *hacking* dapat disebut sebagai kejahatan. Tahap pertama dari *hacking* tidak dapat disebut sebagai kejahatan karena belum dapat dikatakan ada bahaya serius yang mengancam. Tahap kedua sampai keempat, dapat disebut sebagai kejahatan. Tahap kedua merupakan kejahatan yang paling ringan karena dalam tahap ini hanya bersifat masuk atau menyusup dan belum ada unsur destruktif. Tahap ketiga dan keempat sudah mengandung unsur destruktif sehingga akibat yang ditimbulkan lebih buruk dibandingkan dengan tahap kedua.

Penulis berpendapat bahwa tahap kedua sampai keempat merupakan kejahatan, hal ini disebabkan karena beberapa hal, yaitu:

a. Memasuki ruang privat pada situs orang lain bukanlah perbuatan terpuji. Sebuah situs dalam proses komunikasi dengan pihak lain (pihak yang mengakses) sudah menyediakan tempat publik untuk itu. Bagaimana ruang publik itu dikelola dan disajikan, merupakan urusan pengelola situs. Pihak pengakses dapat memberikan saran ataupun kritik terhadap apa yang disajikan itu pada tempat atau alamat yang disediakan oleh pengelola situs. Mengganggu privasi orang merupakan pelanggaran terhadap hak asasi orang lain sehingga menyusup, apalagi dilakukan secara diam-diam betul-betul merupakan tindakan yang tidak didasarkan pada moral yang baik. Jika situs yang disusupi itu adalah milik sebuah instansi pemerintah yang vital seperti militer yang menyimpan data-data penting atau rahasia bahkan sangat rahasia mengenai negara, maka masuk atau menyusup ke dalam situs itu tanpa ijin

merupakan tindakan mata-mata. Dalam konstruksi hukum pidana, tindakan menyusup ini dapat dikategorikan sebagai tindakan memata-matai.

b. Menjelajahi daerah atau ruang milik orang lain tanpa ijin merupakan kejahatan karena menganggu privasi pemilik daerah itu. Jika penjelajahan itu dilakukan dan disertai dengan tindakan destruktif, misalnya mengubah tampilan atau *frontpage* dari suatu situs sudah merupakan perbuatan yang mengacaukan ketertiban umum, misalnya seperti yang terjadi pada situs Pusat Dokumentasi dan Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) ketika pertama kali dihack. Situs yang khusus menyediakan informasi mengenai pelayanan buku atau artikel ilmiah itu *frontpage*nya diganti dengan gambar wanita telanjang. Jika orang yang mengetahui apa itu PDII LIPI, maka tentunya ia akan berpendapat atau minimal ia akan bergumam, mengapa situs PDII LIPI menjadi situs porno, bukan situs pendidikan lagi. Tindakan serupa dapat pula dijumpai dalam situs yang dikelola oleh Departemen Luar Negeri dan ABRI. Tindakan merusak milik orang lain dalam konstruksi hukum pidana sudah merupakan tindak pidana, meskipun kejadian itu membawa akibat dalam pelayanan publik di dunia maya, tetapi kerugian yang timbul dirasakan oleh orang-orang yang ada di dunia nyata.[46]

Tindakan cracker yang berusaha untuk mendapatkan akses yang lebih tinggi (*superuser*) merupakan tindakan yang dapat dikategorikan sebagai tindakan pengambilalihan kekuasaan (kudeta) terhadap kekuasaan yang hanya dimiliki

---

[46] Bandingkan dengan ketentuan pidana yang terdapat dalam Pasal 154 KUHP mengenai kejahatan terhadap ketertiban umum dan Pasal 406 - 412 KUHP mengenai penghancuran atau perusakan barang.

terutama oleh administrator sistem. Dengan menjadi superuser berarti cracker menjadi penguasa jaringan komputer atau situs yang dimasukinya itu

c. Meninggalkan tempat yang telah dimasuki apalagi disertai dengan tindakan menghapus *log file* atau data-data penting lain dalam usaha menghilangkan jejak menunjukkan tindakan yang dilakukan cracker merupakan tindakan tidak bertanggung jawab. Tidak ada penjahat yang menyatakan dirinya bertanggung jawab terhadap perbuatan yang dilakukannya. Secara etis tindakan tidak bertanggung jawab ini bertentangan dengan tuntutan moral yang menekankan kejujuran dan pertanggungjawaban.

Dari uraian tersebut dapat disimpulkan bahwa untuk menentukan apakah *hacking* itu merupakan kejahatan atau bukan, maka harus dilihat dengan menggunakan pendekatan atau perspektif yang telah ditentukan secara umum. Penetapan suatu perbuatan sebagai kejahatan atau bukan merupakan kewenangan dari pembentuk undang-undang, dalam hal ini pemerintah dan Dewan Perwakilan Rakyat (DPR). *Crime is any act that lawmakers designate as "court-punishable behaviour,"* demikian kata **James Levin**.[47] Agar dapat disebut atau dikategorikan sebagai kejahatan, maka harus memenuhi beberapa karakteristik dari tindak pidana, yaitu:

a. Bertentangan dengan atau merugikan kepentingan umum (*a public wrong*). Dilihat dari kriteria ini, maka tindakan *hacking* yang dilakukan oleh cracker sangat bertentangan dan merugikan kepentingan umum bahkan kepentingan pribadi. Seorang cracker yang menyerang situs yang menyediakan pelayanan

[47] James Levin, et.al., *Criminal Justice A Public Policy Approach*, Harcourt Brace Jovanovich, New York. 1980. hal. 63-64.

publik atau menyediakan data-data yang diperuntukkan bagi publik sudah barang tentu merugikan pengakses yang hendak mengakses situs itu, dalam hal ini tidak hanya pemerintah atau perusahaan yang dirugikan (sebagai penyelenggara pelayanan umum) tetapi juga merugikan kepentingan pengakses. Demikian juga dengan situs yang dikelola secara pribadi, jika dihack maka akan menganggu kepentingan dari pemilik situs itu secara pribadi.[48]

b. Bertentangan dengan moral masyarakat (*a moral wrong*). Tidaklah mudah untuk menentukan dasar moral apa yang dipakai sebagai pertimbangan dalam memutuskan suatu perbuatan sebagai kejahatan atau tidak. Dalam hal ini dasar moral yang dipakai tentunya dapat diambilkan dari kehidupan masyarakat sekitar atau di mana perbuatan itu ada atau terjadi (yang berarti kehidupan dalam alam nyata) dan ketentuan-ketentuan moral yang dipakai atau dipergunakan dalam kehidupan para *netizen* (dalam hal ini moral dalam masyarakat yang ada di *cyberspace*). Para *netizen* umumnya mengakui bahwa menghack sebuah situs merupakan tindakan yang tidak baik apalagi jika *hacking* itu dilakukan terhadap situs-situs pendidikan, penelitian dan pelayanan umum.

Untuk membahas lebih lanjut mengenai aspek jahat dari *hacking*, maka akan dilakukan melalui perspektif kriminologi. Untuk memahami *hacking* sebagai kejahatan tentunya tidak cukup dengan hanya mempelajari dari sisi akibat

---

[48] Mengenai perbuatan yang bertentangan dan merugikan kepentingan umum ini, bandingkan dengan pendapat **Sir Carleton Allen** yang menyatakan *"Crime is crimie because it consist in wrongdoing which directly and in serious degree threatens the security or well-being of society, and because it is not safe to leave it reressable only by compensation of the part injured."* J.C. Smith dan Brian Hogan, *Criminal Law*, English Language Book Society/Butterworths, London, 1988, hal. 18.

berupa kerugian-kerugian yang diderita oleh para korban dan landasan atau aturan-aturan apa yang dipakai oleh penguasa atau pembentuk undang-undang untuk menentukan suatu perbuatan sebagai kejahatan. Dalam perspektif teori kriminologi kritis, maka akan dibahas mengenai pergeseran realitas sosial ke realitas virtual, konstruksi sosial dan terakhir analisa berdasarkan teori kriminologi kritis.

Realitas virtual yang ditampilkan dalam *cyberspace* merupakan suatu kenyataan, fenomena yang kehadirannya tidak dapat ditangkap atau dipegang dengan tangan tetapi keberadaannya tidak dapat dielakkan. Keberadaan realitas virtual bukanlah kenyataan yang begitu saja jatuh dari langit (*taken for granted*), akan tetapi keberadaannya itu diadakan atau dikontruksikan secara sosial oleh orang-orang yang bergerak dan menggeluti teknologi informasi. Internet merupakan proses konstruksi tahap demi tahap. Internet menurut pernyataan **Jaron Lanier** merupakan tahap revelasi yang diturunkan secara tahap demi tahap yang akan merentang pada beberapa generasi.[49]

Dunia fisik yang kita tempati sekarang dan dunia yang disimulasi dalam komputer (*virtual life/virtual reality*) secara fundamental terbuat dari hal yang berbeda dan inilah yang menyebabkan yang satu berbeda dengan yang lain. Ini merupakan konsep yang sangat penting. Dunia fisik terbuat dari bahan-bahan alam yang dipahami sebagai partikel atau gelombang atau apapun. Ini merupakan materi yang oleh para ahli fisika terus menerus dipahami dan mungkin tidak akan pernah berhasil. Kita memiliki pengetahuan dunia fisik secara terbatas karena keterbatasan empirisisme, kita selalu semakin dekat

---

[49] Jaron Lanier dalam percakapannya dengan Jeff Zaleski dalam Jeff Zaleski, *loc.cit*, hal. 162

dengannya, namun tidak pernah sempurna. Dunia yang disimulasi terbuat dari progam komputer. Program-program komputer terbuat dari ide-ide. Jadi atom dari dunia virtual berbeda dengan atom dunia fisik. Ia sebetulnya adalah ide, tetapi ide yang sangat akurat.[50]

Web sebutan lain untuk internet memang sudah menjadi tempat yang luas, ia ibarat lautan. Bagi **Jaron Lanier** hal yang paling mengesankan dari *web* adalah untuk pertama kalinya dalam sejarah, kita memiliki anarki yang berhasil baik. Menurutnya, sebagian besar dari kita pernah melewati beberapa fase idealistik ketika kita mengira anarki adalah hal yang mungkin. Web adalah sesuatu yang tidak direncanakan, tanpa figur otoritas, tanpa selebritis, tanpa publikasi luas, bahkan tanpa uang. Tak satupun struktur motivasi tradisional, entah hirarki, keuangan atau kebutuhan, ada di sana. Web bukanlah sesuatu yang dibutuhkan, ia adalah sesuatu yang diinginkan. Berjuta orang bekerja sama membuat hal yang luar biasa hanya karena menginginkannya.[51]

Di dalam *cyberspace* berbagai peristiwa dirangkai, direkayasa dan kemudian disuguhkan kepada umum dan inilah yang disebut *pseudo-event*. *Pseudo-event* adalah kejadian atau peristiwa yang tampaknya terjadi secara spontan, tetapi semuanya terjadi karena seseorang merencanakan, merekaysan atau memprovokasinya. Realitas virtual merupakan produk yang dihasilkan oleh pelaku-pelaku sosial yang berdasarkan ideologi dan kepentingan-kepentingan mengarahkan tindakannya pada tujuan-tujuan yang dikehendaki. Mereka menciptakan realitas seperti apa yang mampu dilakukan dan diinginkan.

---

[50] *Ibid.* hal. 171-172
[51] *Ibid.* hal. 161.

Kejadian-kejadian palsu kini tumpang tindih dengan realitas yang sesungguhnya sehingga publik boleh jadi berspekulasi secara bebas mengenai makna kebenaran.[52]

Cyberspace, yang realitasnya dalah realitas virtual, merupakan dunia yang melampau realitas yang ada, sebuah *hyperreal*, sebuah realitas virtual (*virtual reality*). Dunia realitas yang melampaui dan bersifat artifisial ini menjajah hampir setiap realitas yang ada dan pada suatu hari nanti akan mengambil secara total realitas-realitas tersebut. Dalam dunia posmodern batas antara *event* dan *pseudo-event* tampaknya telah lenyap karena *pseudo-event* telah menjadi kehidupan nyata.

Realitas itu sendiri kini direkayasa sedemikian rupa, sehingga tidak dapat lagi dibedakan antara realitas yang asli dan yang tiruan/representasi (*simulacra*). **Jean Baudrillard** dalam *Simulations* mendefinisikan itulah simulasi (*simulation*) sebagai "... penciptaan model-model kenyataan yang tanpa asal-usul dan realitas: *a hyperreal*. Model-model tersebut memang sepintas tampak nyata akan tetapi ia sesungguhnya tidak menggambarkan kenyataan yang sebenarnya. Ia sebaliknya, menyembunyikan kenyataan yang hakiki. Kenyataan (*real*) ditutupi oleh tanda kenyataan (*sign of the real*) sedemikian rupa sehingga antara tanda dan realitas, antara model dan kenyataan tidak dapat lagi dibedakan. Simulasi tidak menggambarkan realitas sebagaimana adanya, maka realitas yang

---

[52] Ketika kita memasuki dunia realitas virtual, yang kita lihat di sana adalah suatu konstruksi yang dibuat atau disusun oleh para ahlinya. Dunia ini didefinisikan dengan tepat, maka seluruh sisi begitu tajam. Apa yang diserap oleh kita di dunia *virtual* dibuat oleh seseorang, tak lebih dari itu dan tak kurang. Untuk pertama kalinya kita memiliki sisi yang tajam berlawanan dengan sisi yang samar di dunia sehari-hari, dan apapun di dekat sisi yang tajam tersebut, itu adalah kita. Kita tidak akan pernah dapat merasakan hal yang sama dalam realitas fisik pada tingkat yang sama dengan realitas virtual. *Ibid*, hal. 171

dihasilkan oleh simulasi adalah realitas yang melampaui atau *hyperreali*, artinya realitas tersebut tidak dapat lagi dinilai berdasarkan ukuran-ukuran (rasional, moral) yang ada para realitas yang sesungguhnya.[53]

Teknologi informasi yang menghasilkan *cyberspace* dengan dunia simulasinya itu sekarang telah memetik hasilnya. Orang-orang berbondong-bondong menikmati realitas baru yang ditawarkan, duduk berlama-lama di depan layar komputer, menanggalkan segala atribut dan menikmati sajian yang ditawarkan. Realitas virtual telah dianggap lebih menyenangkan dari kenyataan kehidupan sebenarnya karena di sana tidak ada air mata, tidak ada kekerasan yang nyata (meskipun kekerasan virtual itu ada), dan kekerasan atau ancaman kejahatan tidak dapat melukai tubuh karena ketika mengembara ke *cyberspace*, badan ditinggalkan. Dalam pengembaraan itu, yang mengembara adalah ide, pikiran serta gagasan.

Realitas virtual tidak hanya membiarkan kita untuk menikmati realitas yang disajikan (dalam arti pasif, hanya menikmati), akan tetapi ia juga menawarkan kita untuk bermain di dalamnya (dalam arti aktif). Realitas virtual yang di dalamnya terjadi lalu lintas berbagai keperluan manusia dari penjuru dunia itu juga menawarkan berbagai harapan, kemudahan dan juga keuntungan yang dapat diraih tanpa kita menggerakkan anggota badan yang berlebihan seperti seorang pekerja yang dengan keras menggerakkan anggota badan dan otot-ototnya.[54]

---

[53] Yasraf Amir Piliang, *Mesin-mesin Kepalsuan*, Kompas, 14 Juni 2000, versi elektronik dapat diperoleh di http://www.kompas.com/mesi45

[54] *Cyberspace* memang menawarkan keuntungan yang tidak terhingga bagi orang-orang yang mengetahuinya. Optimisme keuntungan yang dapat diraih dari realitas virtual terungkap seperti apa yang pernah diungkapkan oleh **Al Gore** (Mantan Wakil Presiden Amerika Serikat 1993-2001). **Al Gore** pada suatu kesempatan mengatakan bahwa jaringan global Internet akan membawa keuntungan bersama bagi seluruh anggota keluarga umat manusia, misalnya peringatan

Perusahaan-perusahaan yang melihat *cyberspace* sebagai pasar potensial mulai membuka situs untuk melayani para penghuni *cyberspace*. Maka bermunculan *telemarketing* berupa *internet banking, credit card virtual, teleshopping* yang memungkinkan orang untuk belanja tanpa ke toko atau supermarket, cukup memainkan jari-jari di depan layar komputer yang terhubung ke situs perusahaan itu. Pelayanan-pelayanan virtual menjadi trend yang menggejala dalam kehidupan bisnis khususnya dan masyarakat pada umumnya.

Di bidang bisnis, hampir setiap barang yang ditawarkan di toko-toko atau supermarket dapat dijumpai di *teleshopping* ini, bahkan hal-hal yang bersifat pribadi pun ditawarkan. *Cyberspace* dengan realitas virtualnya betul-betul memberi peluang kepada pelaku bisnis untuk memanjakan konsumen dengan segala kemudahan yang ada dan berbagai layanan yang sebelumnya tidak terpikirkan. Dalam dunia politik, para politisi juga bisa memanfaatkan *cyberspace* sebagai media komunikasi antara pengikut partai dengan pemimpin partainya, sebagai media pendidikan politik, propaganda visi dan misinya serta berbagai keperluan lain yang terkait dengan politik. Internet menjadi media yang cukup ampuh untuk menyuarakan pendapat politiknya, mencerca lawan politiknya dan menumbuhkan kebebasan berpendapat menuju kehidupan demokrasi.

---

dini terhadap bencana alam, peningkatan kesehatan, pendidikan yang lebih baik, pemecahan masalah lingkungan hidup, informasi pasar yang semakin luas dan penyebaran demokrasi. Keoptimisan **Al Gore** kembali terungkap dari pernyataannya yang menjamin teknologi informasi itu akan meningkatkan pertumbuhan ekonomi, mengembangkan demokrasi dan "menjadikan setiap orang di seluruh dunia saling terhubung", memandikan kita semua, mau tak mau (seperti ibu memandikan anaknya) dengan susu hangat kebajikan manusia. Satu dunia, satu kasih.Mark Slouka, op.cit., hal. 116. Lihat juga pernyataan Al Gore dalam *Speech at the Superhighway Summit Royce Hall*, 11 Januari 1993, UCLA Los Angeles, California, versi electronik dapat dijumpai di http://www.eff.org/pub/GII_NII/Govt_docs/gore_shs.speech, seperti yang telah diungkapkan dalam bab sebelumnya.

Para *netizen* dimanjakan dengan berbagai informasi dari koran dari dalam maupun luar negeri tanpa membeli koran itu, menikmati musik tanpa harus membeli kaset bahkan dapat menikmati hiburan yang menyegarkan tanpa harus ke kafe, bioskop ata tempat hiburan lainnya. Para peneliti yang memanfaatkan internet dimanjakan dengan berbagai literatur yang tersaji secara gratis tanpa harus mengeluarkan uang untuk pergi ke tempat informasi berada. Para budayawan dan sastrawan melihat dunia yang satu ini sebagai dunia yang penuh harapan dengan menyebarkan ide-ide melalui bit-bit komputer dan menyebar sendiri melalui internet. Tidak ketinggalan para religionis atau spiritualis menggunakan internet untuk menjumpai umatnya seperti umat kristiani yang menuju keuskupan maya **Partenia**.[55]

Keadaan-keadaan seperti itulah yang menurut **John Naisbitt, Nana Naisbitt** dan **Douglas Philips** disebut Zona Mabuk Teknologi, di mana orang berbondong-bondong memanfaatkan teknologi (dalam hal ini teknologi informasi) karena teknologi itu sendiri berikrar akan membuat hidup lebih baik, membuat kita lebih pintas, meningkatkan kinerja kita dan membuat kita bahagia. Teknologi berjanji akan lebih cepat, lebih murah dan lebih mudah daripada segala sesuatu yang sudah pernah ada. Teknologi berjanji akan menghubungkan kita dengan dunia luar, namun tetap menjaga kita agar tetap dekat dengan para sahabat dan keluarga yang kita cintai. Ia juga berjanji menjadi landasan ekonomi

[55] Partenia merupakan keuskupan katolik maya yang dibuat oleh Galliot untuk menyebarkan Injil ke dunia maya. Berdiri pada 13 Januari 1996. Galliot dengan komputer pinjaman melompati jurang daru dunia nyata ke dunia maya dengan memindahkan Partenia (yang sebenarnya sebuah tempat di Afrika Utara) ke *cyberspace*. Situs pelayanan Partenia dapat dijumpai di http://ww.partenia.org

dunia yang baru dan penyeimbang yang kuat, dan menjadikannya kita kaya serta janji-janji lain yang tak ada habisnya.[56]

Perkembangan *cyberspace* telah membawa beberapa pengaruh sosial, politik, budaya dan etika yang sangat besar terhadap masyarakat atau komunitas baru yang diciptakannya. Orang semakin hari semakin menyenangi dunia baru ini, merasa betah dan nyaman di dalamnya dan menganggap dunia maya ini sebagai alam kedua mereka. Mereka menyenangi *cyberspace* karena dapat menggantikan ruang publik (*public space*) yang telah semakin menghilang di dalam masyarakat kita karena telah diganti dengan bangunan bertingkat, lapangan golf, pusat perbelanjaan dan sebagainya.

Kebebasan yang didapat di *cyberspace* terkadang tidak dapat dinikmati di dunia nyata, sehingga banyak orang berbondong-bondong masuk ke *cyberspace*. Inilah yang dikatakan bahwa realitas virtual akan menggeser kehidupan nyata sehubungan dengan keterbatasan yang dimiliki kehidupan nyata. Realitas virtual memecahkan kebuntuan yang dimiliki kehidupan nyata mengenai konsep ruang dan waktu. Realitas virtual memungkinkan orang yang ada di dalamnya berada pada tempat dan waktu yang berbeda. Inilah ruang yang

---

[56] Zona Mabuk Teknologi merupakan zona yang ditunjukkan oleh adanya hubugan yang rumit dan seringkali bertentangan antara teknologi dan pencarian kita tentang makna. Gejala Zona Mabuk Teknologi adalah:
1. Kita lebih menyukai penyelesaian masalah secara kilat, dari masalah agama sampai gizi
2. Kita takut sekaligus memuja teknologi
3. Kita mengaburkan perbedaan antara yang nyata dan yang semu
4. Kita menerima kekerasan sebagai sesuatu yang wajar
5. Kita mencintai teknologi dalam wujud mainan
6. Kita menjalani kehidupan yang berjarak dan terenggut.

John Naisbitt, Nana Naisbitt dan Douglas Philips, *High Tech High Touch, Pencarian Makna Di Tengah Perkembangan Pesat Teknologi*, Mizan, Bandung, 2001, hal. 21, 23-24

memberikan kekuasaan kepada setiap orang, bukan segelintir orang, sebuah tempat yang lebih baik untuk membuat semua orang bahagia di setiap waktu. Semakin maju teknologi virtual, semakin lebih baik kondisi kehidupan global dan inilah optimisme terhadap jagat raya *cyberspace*.

Optimisme terhadap *cyberspace* bukan tanpa korban. Ia menimbulkan korban berupa realitas itu sendiri. Pergeseran yang menyebabkan orang-orang lebih mempercayai realitas semu yang ditawarkan oleh *cyberspace* daripada realitas sosial beserta kearifan yang telah dibangun beberapa lama. Proses *cyberisation* telah menyebabkan masyarakat kehilangan realitas masa lalu dengan kearifan yang tersimpan di dalamnya yang sebenarnya lebih berharga bagi pembangunan manusia itu sendiri, seperti rasa kedalaman, kebersamaan semangat spiritualitas, ikatan moralitas, semangat komunitas dan semangat solidaritas.

Berjuta harapan muncul dalam benak penikmat dan penduduk *cyberspace*, di sisi lain berjuta masyarakat khawatir dengan perkembangan *cyberspace* dan telah menjadi ancaman bagi realitas itu sendiri. Di antara orang-orang yang menikmati harapan-harapan yang telah terpetik dari *cyberspace*, terdapat orang-orang yang melihat *cyberspace* sebagai ancaman dan secara berlahan-lahan membangun kembali realitas dunianya yang penuh dengan kearifan dan kebijakan-kebijakan yang tidak di dapat di *cyberspace*.

Para penolak budaya *cyberspace*, terutama **Mark Slouka**, mengecam dengan tajam perubahan yang terjadi akibat kehadiran *cyberspace* dan memprihatinkan kehidupan nyata yang semakin ditinggalkan. Dengan

mendasarkan diri pada pendapat beberapa orang.[57] **Yasraf Amir Piliang** menyimpulkan menjadi beberapa point penting dari mereka yang menolak realitas *cyberspace*. Mereka menolak cyberspace karena cyberspace dilihat sebagai abad yang penuh bahaya, penuh ancamanan,[58] menyuguhkan berjuta kepalsuan, berjuta kesemuan,[59] berjuta ketidakpedulian. Mereka mencurigai realitas virtual hanya dijadikan sebagai alat politik oleh kekuatan *superpower* (khususnya Amerika Serikat) dalam upaya mempertahankan hegemoni politik, ekonomi dan budayanya. Apa yang terjadi sebenarnya adalah proses *Amerikanisasi* yang dipermudah dengan bantuan teknologi realitas virtual. Demokrasi global dan kebebasan yang ditawarkan[60] dalam *cyberspace* sesungguhnya lebih tepat disebut representasi demokrasi, yang mayoritas masyarakat dunia menikmati citra partisipasi mereka di dalam keputusan-keputusan yang menentukan hidup mereka, akan tetapi keputusan-keputusan penting tetap saja dibuat oleh para elit: borjuis, politisi, birokrat dan pakar.

---

[57] Pendapat-pendapat yang menjadi dasar dari kesimpulan ini di antaranya adalah pendapat yang dikemukakan oleh Howard Rheingold dalam *The Virtual Community*, James Brook dan Iain A. Boal dalam *Resisting Virtual Life: The Culture and Politics of Information*, Mark Slouka dalam *War of the World: The Assault on Reality* dan Paul Virlio, *The Aesthetics of Disappearance*. Yasraf Amir Piliang, dalam Mark Slouka, *op.cit.*, hal. 22-25

[58] Sifat bahaya ini nampak dari apa yang dikatakan oleh **Jean Baudrillard** dalam Simulation, citra simulasi justru dianggap lebih mempesona dan superior oleh manusia posmodern ketimbang yang alamiah. Ketika dunia virtual lebih menyenangkan daripada dunia nyata, komputer menjelma menjadi jendela kita menuju dunia, menggantikan jendela rumah kita yang sesungguhnya, yang melaluinya sahabat kita datang berkunjung. Mark Slouka, *op.cit.*, hal. 21, 24-25

[59] Sifat kesemuan semakin menampakkan dirinya ketika realitas virtual menjelma menjadi alat bagi perkembangbiakan kapitalisme global. Sebagaimana dikatakan oleh **James Brook** dan **Iaian Boal**, orang-orang dapat memperoleh perangkat keras, perangkat lunak, hiburan dan pelayanan informasi dan diberi imbalan dengan ilusi kekuasaan. Untuk sebagian besar penduduk dunia, abad informasi dan revolusi komputer berarti semakin tergradasinya kondisi kehidupan, sebuah kondisi yang di dalamnya manusia tak lebih dari sekumpulan budak dan hamba sahaya. *Ibid*, hal. 21-22

[60] *Cyberspace* menjelma menjadi sebuah dunia anarkis yang menakutkan, sebuah dunia yang di dalamnya kebebasan diartikan sebagai kebebeasan untuk mencaci maki dan menyakiti, kebebasan percakapan cabul lewat telepon (*party line*) yang anonim. Orang-orang di dalam *cyberspace* menenggelamkan diri dalam sifat anarki yang abstrak, bebas mempertontonkan apa saja kepada orang lain tanpa rasa malu, mencaci orang tanpa rasa bersalah dan bebas memalsukan apa saja tanpa rasa berdosa. *Ibid.* hal. 22 dan 24

Selain hal tersebut, realitas virtual dipandang bersifat sangat agresif dan destruktif.[61] Ia menyerang apa saja yang kita miliki, ia membunuh apa saja dari diri kita yang sangat berharga. realitas virtual tidak mampu meningkatkan nilai kita sebagai manusia sebagaimana yang dijanjikan. Ia menjadikan kita terperangkap di dalam sebuah dunia yang menjadikan diri kita *sebagai the silent majorities*. **Slouka** tidak menolak sepenuhnya dunia realitas virtual, yang ia tolak adalah sikap arogan para pakar dan penganutnya (*net religionist*).[62]

Dunia realitas virtual disarati oleh trik-trik citraan, tetapi kita menerima citraan tersebut sebagai realitas, tanpa menyadari trik-trik visual tersebut. Trik-trik di dalam representasi komputer sebagaimana dikatakan **Paul Virlio**, dapat menjadikan sesuatu yang supernatural menjadi realitas. Akibatnya fotografi (sebagai sebuah bentuk visual, representasi dari dunia nyata) tidak dapat sepenuhnya lagi dipercaya sebagai gambaran realitas karena ia telah menjelma menjadi simulasi realitas.[63]

Bagi para pengkritik *cyberspace*, realitas hanyalah suatu kebiasaan, sebuah cara berfikir, semuanya hanyalah informasi. "Realitas telah mati" demikian kata **Benedikt** yang menggambarkan *cyberspace* sebagai sebuah wilayah yang dihuni oleh data dan kepalsuan, pikiran dan kenangan tentang alam, sejuta suara dan dua juta mata, menyapu bak gelombang berkilauan, berdengung-

---

[61] Realitas virtual secara brutal menyerang nilai-nilai moral, yang menyebabkan segala batas-batasnya. Realitas virtual, dengan menyuguhkan ke hadapan kita realitas yang tercabut dari dunia, dari batas-batas dan tanggung jawab, menciptakan sebuah dunia amoral karena batas antara baik dan buruk, benar dan salah, asli dan palsu seakan-akan telah lenyap. *Ibid*, hal. 23

[62] Para pakar dan penganutnya percaya bahwa:
a. segala persoalan manusia dapat dipecahkan oleh teknologi realitas virtual
b. setiap dunia fisik dapat di*download* ke dalam komputer; dan
c. masa depan umat manusia bukan di dalam *real life*, melainkan di dalam *virtual life*.
Inilah orang-orang yang bekerja super keras dalam merekayasa kehancuran diri mereka sendiri (*global self destruction*); *Ibid.*

[63] *Ibid*, hal. 25

dengung, mengalir, sebuah perpustakaan *Borges*, sebuah kota; intim, kukuh, cair, dapat dikenali sekaligus tidak.[64]

Menurut **Slouka** dalam rangka memahami revolusi digital sepenuhnya, kita perlu benar-benar mengetahui dua hal dengan jelas, yaitu:[65]

a. Komputer yang bukan sekadar pengolah informasi, tetapi sedang berkembang menjadi mesin peniru canggih, memiliki kemampuan yang kian meningkat untuk meniru aspek-aspek tertentu dari kehidupan kita.

   Komputer sebenarnya tidak ada, demikian kata **Jaron Lanier**. Komputer hanyalah seonggok materi dan ia berfungsi sebagai komputer karena adanya kemampuan kultural untuk mengenal fungsi sebagai komputer. Jadi kita dapat menjadikannya sesuai dengan keinginan kita, dan semua penafsiran sahihnya dengan penafsiran yang berbeda terhadap simbol-simbol jika kita membuat bahasa baru. Untuk menafsirkan komputer ada beberapa pilihan. *Pertama*, ia adalah saluran penghubung antar manusia. Ia adalah teknologi komunikasi yang di dalamnya banyak orang dapat membuat dunia miniatur yang memodelkan segala sesuatu. Semua itu agar ia memiliki bentuk baru komunikasi yang di dalamnya mereka menyusun realitas obyektif bersama dalam bentuk simulasi, bukan sekadar memindahkan simbol-simbol antar mereka secara ekslusif. Kedua adalah dengan menganggap mereka sebagai entitas lain yang menyerupai manusia. Sekarang ini menjadi masalah yang sangat serius dan masalahnya di sini adalah apakah kita memperhatikan

---

[64] Michael Benedikt, *Introduction*, dalam Michael Bendikt (ed), *Cyberspace*, Cambridge, Mass: MIT Press, 1991, hal. 2

[65] Mark Slouka, *op.cit.*, hal. 62

betapa ajaibnya hidup ini atau tidak. Pengalaman langsung mengenai hidup adalah sesuatu yang misterus dan sangat luar biasa.[66]

b. Sejumlah besar orang-orang jenius dan berpengaruh, percaya bahwa komputer harus dan akhirnya akan menggusur dunia asli yang telah berhasil diimitasikan itu.

Sebegitu dahsyatnya serbuan teknologi informasi terhadap realitas hingga menyebabkan **Mark Slouka** menyebutnya sebagai ilusi yang begitu sempurna, yang akan membodohi kita, membuat kita menyangka ilusi itu yang sebenarnya, seperti seekor burung yang menabrak kaca jendela. Genggaman kita pada realitas objektif tempat kita bergantung sudah hampir lepas, kaki kita senantiasa diberati oleh timbunan hal-hal yang bukan realitas yang kita santap schari-hari. Ilusi yang ditawarkan dalam dunia simulasi bisa juga merupakan kebohongan, tetapi seperti dikatakan **Adolf Hitler**, kebohongan (dalam konteks ini adalah kepalsuan sebagai wujud dari simulasi), jika dipropagandakan dan diulang-ulang dalam intensitas yang cukup akan menjadi kebenaran itu sendiri.[67]

Kritik dan kecemasan terhadap perkembangan *cyberspace* dengan realitas virtualnya dapat saja dikemukakan, tetapi hal ini tidak akan menghalangi perkembangan teknologi informasi yang semakin hari semakin menunjukkan

---

[66] Jaron Lanier dalam Jeff Zaleski, *op.cit.*, hal. 164-165.

[67] Dalam bagian akhir dari tulisannya, **Mark Slouka** mengungkapkan bahwa apa yang baik bagi bisnis belum tentu baik bagi kebudayaan. Revolusi digital mungkin baik bagi bisnis, namun dari beberapa sudut pandang kebudayaan, ini berita buruk. Revolusi digital adalah berita buruk, setidak-tidaknya karena ia adalah produk globalisme. Pada satu sisi globalisme memang patut dikagumi, sebagai metafora toleransi dan efektif sebagai strategi pemasaran, akan tetapi pada sisi lain globalisme adalah abstraksi yang terlalu luas dan kabur bagi kebanyakan orang karena manusia seperti halnya spesies lain memang lebih bersifat lokal daripada global. **Mark Slouka** kecewa terhadap revolusi digital karena revolusi digital hanya menawarkan sedikit tetapi menuntut terlalu banyak. Apa yang ditawarkan adalah informasi (dan lebih banyak informasi) serta suatu jenis keterhubungan baru yang abstrak dan yang harus kita bayarkan adalah kesetiaan kita terhadap dunia fisik, mengalihkannya ke dunia maya. Ini transaksi yang buruk, tidak hanya karena dia mengabaikan kebutuhan-kebutuhan biologis kita, tetapi karena dia pun membatasi otonomi kita. Mark Slouka, *op.cit*, hal. 143, 153 dan 167

sebagai kekuatan yang menakjubkan. Di kalangan para *cyberis* sejati (seperti **John Perry Barlow**), semakin tinggi saja kecenderungan untuk mengklaim bahwa berkat komputerlah segala sesuatu bisa maju. Di mata teoritikus *cyberspace*, seperti **Nicole Stenger**, menghabiskan waktu di *cyberspace* akan mengubah kepekaan kita terhadap cahaya, terhadap kedalaman, membuat mimpi-mimpi kita cemerlang dan memudahkan penggunaan metafora dalam berbahasa, melahirkan euforia dan menumbuhkembangkan intuisi. Tetapi diingatkan oleh **Stenger** bahwa kekuataan penjelmaan dan pengetahuan ini akan dirasakan sebagai pelecehan moral yang sangat serius oleh banyak orang sebab kebebasan berimajinasi ditakuti oleh penguasa karena *cyberspace* adalah sama dengan kebebasan berimajinasi itu sendiri.[68]

Realitas yang ditawarkan melalui *cyberspace* (terlepas dari pro dan kontra yang mengiringinya) telah memberikan nuansa baru pada berbagai sisi kehidupan. Berbondong-bondong orang bermigrasi ke sana, dengan meninggalkan badan tentunya dan menjadi warga *cyberspace*. Menjadi warga *cyberspace* yang tidak memerlukan birokrasi untuk mendapatkan Kartu Tanda Penduduk (KTP) maupun Kartu Keluarga, juga tidak perlu bersusah-susah untuk mendapatkan akses pada sebuah situs yang letaknya secara geografis sangat tidak mungkin dijangkau hanya dalam beberapa menit saja.

Sebagaimana kehidupan nyata, dinamika *cyberspace* juga diisi oleh berbagai orang dengan sifat dan perilakunya yang menguntungkan dan juga merugikan. Pada umumnya, mereka yang memandang *cyberspace* dengan penuh

---

[68] Stenger mengingatkan Hitler maupun Stalin dikenal sebagai penguasa yang melarang penerbitancerita dongeng. *Cyberspace* adalah ranah bagi imajinasi, totaliterianisme membenci imajinasi, maka siapapun yang menentang *cyberspace*, berarti memiliki tendensi totaliterianisme. Nicole Stenger, Mind is Leaking Rainbow, dalam Michael Benedikt (ed), *op.cit.*, hal. 57

harapan keuntungan memanfaatkan kehadiran *cyberspace* sebagai tempat untuk bergerak dalam berbagai hal, seperti bisnis, politik, hiburan, penelitian dan juga pendidikan. Pada sisi lain ada juga yang berpendapat *cyberspace* merupakan tempat untuk melakukan kejahatan, sebagai media baru melakukan aksi jahatnya. Mereka inilah yang disebut *cracker* dan dalam perspektif realitas sosial kejahatan, cracker semakin menunjukkan asumsi bahwa masyarakat mempunyai penjahatnya sendiri.

Kejahatan merupakan fenomena sosial sebagai rangkaian dari keseluruhan proses-proses sosial, budaya, politik, ekonomi dan struktur yang ada di dalam masyarakat. Hasil akhir yang tercipta dari proses-proses merupakan hasil sejarah hubungan antar manusia dan untuk selanjutnya ikut mempengaruhi hubungan antar manusia. Dengan demikian untuk memahami masalah kejahatan menurut **I.S. Susanto**, perlu diperhatikan keseluruhan proses-proses yang terjadi di dalam masyarakat mengingat pengertian kejahatan bersifat relatif dan jauh dari pengertian absolut.[69] Untuk itulah analisa dengan menggunakan paradigma kriminologi kritis diperlukan dalam hal ini, karena penentuan jahat atau tidaknya suatu perbuatan tidak hanya ditentukan oleh kerugian-kerugian yang diderita oleh korban tetapi penentuan itu ditentukan juga oleh proses-proses yang terjadi di masyarakat.

Dengan mendasarkan pada teori realitas sosial kejahatan dari **Richard Quinney**, maka keberadaan cracker sebagai penjahat dapat dianalisis sebagai berikut. Sejarah teknologi informasi membuktikan bahwa lahirnya internet

---

[69] I.S. Susanto, *Statistik Kriminal Sebagai Konstruksi Sosial (Penyusunan, Penggunaan dan Penyebarannya, Suatu Studi Kriminologi)*, loc.cit, hal. 1.

merupakan ide, gagasan yang dibuat untuk kepentingan sebuah kekuatan yang sangat besar waktu itu, yaitu kekuatan militer Amerika Serikat. Internet dibangun untuk mengembangkan lingkungan maya sebagai tempat pelatihan militer skala besar dan menyelamatkan berbagai informasi penting negara apabila perang dingin antara Amerika dan Uni Sovyet pecah. Internet dianggap sebagai tempat yang aman untuk menyalurkan informasi penting itu.

Seiring dengan perkembangan waktu, ternyata perang dingin itu tidak jadi pecah, dan penggunaan internet dialihkan untuk keperluan lain. Amerika sebagai pelopor dalam hal ini pertama-tama menggunakan internet sebagai media pendidian dan penelitian, sehingga tidak mengherankan perkembangan internet marak di berbagai universitas di Amerika. Tampaknya pemerintah Amerika memandang internet merupakan media yang bagus untuk melakukan propaganda politik, menyebarkan idealisme demokrasi dan budaya Amerika ke seluruh dunia secara lebih mudah atau disebut juga proses *Amerikanisasi*.

Para pemimpin Amerika menganut kepercayaan pentingnya pengendalian informasi untuk mendapatkan keuntungan global yang maksimal. Kepercayaan ini diperkuat dengan adanya globalisme yang sangat bagus untuk menyusun strategi pemasaran. Amerika Serikat merespon dan mempelopiri abad informasi ini dengan mengubah paradigma ekonominya dari ekonomi yang berbasis manufaktur ke ekonomi uang berbasis jasa *(from mamifacturing-based economy to a service-based economy)*. Perubahan ini ditandai dengan berkurangnya peranan traditional *raw materials* dan semakin meningkatnya peranan *raw material of a service-based economy* yakni informasi dalam

perekonomian Amerika.[70] Dalam perkembangannya tidak hanya pemerintah Amerika yang berpandangan demikian karena negara-negara lain juga memandang internet sebagai sumber daya yang dapat dan sangat efisien untuk menyebarkan berbagai hal dan memberikan keuntungan yang cukup besar bagi kehidupan perekonomiannya.

Bukti bahwa pemerintah (terutama Amerika Serikat) telah menggunakan internet sebagai alat politik adalah ketika **Al Gore** mencalonkan diri sebagai Presiden pada Pemilu tahun 2000. Ia menggunakan teknologi informasi sebagai alat untuk propaganda politik untuk memenangkan pemilihan presiden. Selain itu pernyataan-pernyataan **Al Gore** sebelumnya menunjukkan optimisme dia terhadap masa depan teknologi informasi.

Internet dalam dunia politik telah menjadi sarana untuk menyerang negara lain. Hal ini ditunjukkan oleh cracker-cracker yang tergabung dalam *hacker Porto* yang menyerang situs-situs milik pemerintah Indonesia dalam perjuangannya memerdekakan Timor-Timur. Perang digital[71] juga terjadi antara Cina dan Amerika yang dipicu oleh pemboman Kedutaan Besar Cina di Beograd

---

[70] Lihat dalam Charles Brill, *Legal Protection of Collections of Facts*, Computer Law Review and Technology Journal, 1998 (Spring), hal. 1. Lihat pula Atip Latifulhayat, *Legal Protection of Databases And Its Implications For Indonesian Law Relating to Intellectual Property Rights*, Thesis in Monash University, Australia, 2000, hal. 1

[71] Pemanfaatan internet untuk perang digital merupakan fenomena yang menarik. Dengan menggunakan strategi perang **Sun Tzu, Onno W. Purbo** menggambarkan bagaimana karakteristik perang digital itu. **Sun Tzu** menyadarkan kita bahwa tidak ada yang terlalu istimewa bagi TNI memperoleh ratusan kemenangan di medan tempur yang bersimbah darah. Adalah prestasi luar biasa jika mengalahkan musuh tanpa perlu bertempur sama sekali. Penguasaan pikiran, budaya, pengetahun merupakan kunci utama keberhasilan bertumpu pada teknik *psychological warfare, netdynamic* berbasis *psychoanalitic* merupakan tingkat yang lebih tinggi daripada sekadar *information warfare* biasa. Perang digital atau perang e-millenium tidak akan terlihat oleh aparat TNI walaupun dengan paradigma reformasi sekalipun. Pertahanan semesta di domain pengetahuan menjadi kunci keberhasilannya. Massa *knowledge based society* merupakan *warfighter* di era *e-millenium*. Onno W. Purbo, *Cyberlaw: Filosofi "Hukum" Di Dunia Maya*, Makalah pada Seminar Nasional Cyberlaw, diselenggarakan oleh STH Bandung, 9 April 2001, tanpa halaman

oleh Amerika Serikat pada Mei 1999 dan persoalan pesawat mata-mata Amerika yang memasuki wilayah Cina pada April 2001. Pertentangan antara Israel dan Palestina juga telah merambah dunia maya. Keduanya saling serang pada situs-situs yang mereka kelola. Mereka telah mengobarkan perang lewat dunia maya. Selain Amerika, Cina, dan Indonesia, masih banyak negara-negara yang memanfaatkan internet dan menjadi korban dari aktivis internet.

Pemanfaatan internet untuk kepentingan politik tidak hanya dilakukan di Amerika, Cina dan Indonesia, kejadian di belahan dunia lain hal juga terjadi, seperti yang dialami oleh Rumania. Internet digunakan untuk mencari dan menjaring dukungan bagi calon presiden Rumania **Ion Illiescu**, meskipun situs yang dibukanya kemudian di*hack* oleh orang lain, tetapi hal ini sudah menunjukkan bahwa internet merupakan sarana yang cukup baik untuk berpolitik. Indonesia, meskipun tertinggal dalam bidang teknologi informasi, dalam hal pemanfaatan teknologi tidak mau ketinggalan, terbukti dengan dibukanya beberapa situs milik pemerintah yang digunakan untuk pelayanan umum.

Tidak hanya bidang politik dan militer serta pendidikan dan penelitian yang memonopoli penggunaan internet, seiring dengan perkembangan ekonomi dunia, internetpun mulai dimanfaatkan sebagai media pemasaran. Kalangan bisnis mulai menginginkan sistem perdagangan global yang cepat, didukung oleh komunitas digital dengan tingkat kepercayaan yang tinggi. Sistem perdagangan yang dilakukan selama ini (secara *face to face*) oleh pelaku usaha dengan rekannya di luar negeri dinilai tidak efisien, membutuhkan waktu yang lama,

sehingga perdagangan melalui internet (*e-commerce*) dinilai dapat mengurangi ketidakefisienan sistem perdagangan tradisional.

Globalisme dan globalisasi menyebabkan strategi pemasaran berubah dan internet adalah salah satu alat sebagai media pemasaran. Internet tidak lagi menjadi monopoli pemerintah, internet merupakan tempat orang menggali keuntungan terutama oleh pengusaha atau perusahaan-perusahaan besar yang mampu membeli peralatan jaringan komputer (hardware dan software) serta mampu membayar orang-orang yang ahli untuk menjalankan bisnis di internet. Pada taraf ini, pemerintah dan pengusaha merupakan kelas dominan yang dapat memperoleh keuntungan dari kehadiran internet.

Keuntungan yang dapat diraih oleh kedua pemain besar (negara dan korporasi) dalam internet itu kemudian menyebar pada tiap-tiap individu yang mau dan mampu bermain (dengan segala resiko yang ada) di dunia maya, apalagi setelah internet menjadi begitu familiar bagi setiap orang sejak diketemukannya *World Wide Web* dengan *Hypertext Mark up Languange*. Meskipun demikian pemerintah dan perusahaan tetap memperoleh keuntungan yang besar karena didukung oleh struktur dan infrastruktur yang kuat.

Mengaitkan teknologi informasi hanya dengan dunia politik tampaknya terlalu berat sebelah, meskipun keputusan-keputusan yang diambil pada bidang lain terkadang dipengaruhi oleh ideologi politik dari pembuat keputusan, seperti yang terjadi pada Konferensi Tingkat Tinggi (KTT) G8 pada tanggal 22 Juli 2000 di Okinawa, Jepang. Hasil konferensi yang dilakukan oleh sekumpulan negara-negara maju menunjukkan hegemoni mereka terhadap dunia perekonomian. Dari hasil konferensi itu sebenarnya mereka menunjukkan dominasi mereka di bidang

teknologi informasi dan mengajak negara-negara berkembang dan terbelakang untuk mulai memanfaatkan teknologi informasi.

Bagi mereka (negara-negara peserta KTT G 8), negara-negara berkembang dan terbelakang adalah pasar potensial untuk produk-produk teknologi informasi mereka. Dengan struktur dan infrastruktur perekonomian yang telah dibangun, diperkuat dengan adanya globalisme dan globalisasi, negara-negara maju mulai memanfaatkan forum itu untuk kepentingan politik dan ekonominya. Deklarasi Okinawa yang dihasilkan dalam KTT tersebut sebenarnya merupakan eufemisme untuk menunjukkan keinginan mereka mengekspor teknologi informasi ke seluruh dunia yang berarti devisa baginya. Dengan kata lain ujung dari Konferensi Tingkat Tinggi itu adalah keuntungan, keuntungan yang akan diperoleh dari eksploitasi teknologi informasi.

Sinyalemen seperti itu tampak dari apa yang dikemukakan oleh **Al Gore** seperti di bawah ini:[72]

> The principles comprising our vision have provided a template for development of the Global Information Infrastructure (GII) in countries widely varying needs, cultures and technologies. In the developing world, we are promoting and supporting telecommunications development through these *principles as an essential factor in economic growth and development*, and not as a luxurious result of growth. To our economic competitors and trading partners, we have laid out a challenge to remove our remaining barriers to foreign investment in telecommunications services as they do the same.
> In all cases, global and national development are not possible without allowing private investment *open access to the marketplace, and competition - and we are fighting to achieve this around the world.*

Harapan untuk mengais keuntungan dari teknologi informasi ini juga tercermin dari pendapat **Al Gore** yang lain, yaitu[73]

---

[72] Al Gore. *Bringing Information to the World: The Global Information Infrastructure*, Harvard Journal of Law & Technology 1 (Winter 1996)

[73] *Ibid.*

> President Clinton understands how important a balanced budget is to our economic future. He also understands how critical these technology investment are to ensuring future economic growth. That is why he balanced his budget in away that preserves the nation's leadership in science and technology

Keuntungan yang ingin didapat dari bisnis teknologi informasi ini ternyata tidak selamanya mulus, terbukti dari hasil survei yang dilakukan oleh *American Society for Industrial Security* pada tahun 1996 menunjukkan adanya kerugian akibat pelanggaran *intellectual property*. Potensi kerugian yang terjadi di seluruh Amerika adalah lebih dari $63 billion yang berarti tiap bulan rata-rata mengalami kerugian sebesar $5,25 billion. Era informasi ternyata membuat *access* lebih mudah untuk melakukan kejahatan dan hal ini kemungkinan akan berlanjut dan frekuensinya akan meningkat.[74]

Apa yang diinginkan oleh setiap orang tidak selamanya dapat menjadi kenyataan, demikian pula harapan-harapan yang dibebankan kepada teknologi informasi itu sendiri. Realitas virtual yang ditawarkan tidak selamanya memberikan keuntungan yang diharapkan. Realitas virtual seperti halnya pendapat **Jaron Lanier** merupakan hasil konstruksi, dan pada sisi lain memberikan pula kesempatan untuk membuat kontra konstruksi terhadap realitas virtual itu. Para penghuni *cyberspace* (penikmat dan pemanfaat realitas virtual) yang disebut *netizen* itu bukanlah kumpulan orang-orang yang dapat dengan mudah disetir, dikomando untuk kepentingan para penguasa (untuk kepentingan politiknya) atau pengusaha (untuk kepentingan bisnisnya).

---

74 Lihat lebih lengkap di Neil J. Gallagher, Statemen of the Record on *Cybercrime, Transnational Crime, and Intellectual Property*, March 24, 1999, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress08.htm. Bandingkan dengan Laporan FBI 1999 yang menyebutkan bahwa Departemen Pertahanan Amerika setiap hari menerima 80 - 100 hacking dan virus yang menimbulkan kerusakan dan hilangnya keuntungan bisnis sebesar $7 bilion untuk tiga bulan pertama pada tahun 1999. Lihat lebih lengkap pada Ann K. Moceyunas, *Computer Hacking: A New Warfare*, Net Law News, Oct-Nov-dec 1999.

Para penghuni *cyberspace* juga ingin berkreasi, mandiri dan tidak ingin dipengaruhi oleh kepentingan politik maupun bisnis. Mereka ingin menikmati realitas virtual yang ditawarkan meskipun untuk hal itu mereka harus menembus batas-batas hukum, moral dan etika yang diperbolehkan. Bagi mereka berkelana di *cyberspace* merupakan kenikmatan tersendiri, dapat menembus dan merusak situs milik perorangan atau publik merupakan kebanggaan, dan dalam pandangan mereka kejahatan (*hacking*) adalah candu (selama belum tertangkap).

Cyberspace adalah dunia informasi, dunia yang penuh dengan informasi baik yang akurat maupun informasi sampah. Kebebasan mendapatkan atau menikmati informasi merupakan hal yang didambakan oleh setiap *netizen* atau *virtual community*, tetapi halangan tentu saja ada seperti yang dikemukakan oleh **Mitchell Kapor** pendiri *Electronic Frontier Foundation*,

> Our society has made a commitment to openness and to free communication. But if our legal and social institutions fail to adapt to new technology, basic access to the global electronic media be seen as a privilege, granted to those who play by the strictest rules, rather than as a right held by anyone who needs to communicate.[75]

Bagi pemerintah dan pengusaha (dan kelas dominan lainnya dalam kehidupan cybaerspace), apa yang dilakukan oleh penduduk *cyberspace* yang dikelompokkan dalam kategori cracker ini merupakan ancaman terhadap misi dan visi mereka membangun internet. Mereka merupakan ancaman yang serius dan dapat meruntuhkan dominasi mereka di dunia maya serta mengurangi harapan-harapan yang telah mereka sebarkan dan tanamkan kepada para pengikutnya.

Cyberspace, sebagai dunia yang penuh impian, harapan dan angan-angan dengan realitas virtual yang ditawarkan serta kecemasan-kecemasan yang

---

[75] Mitchell Kapor, *Civil Liberties in Cyberspace: When does Hacking Turn From an Exercise of Civil Liberties into Crime?* Scientific American, September 1991.

menghantui dan disebarkan oleh para pengkritik proses *cyberisation* ini akan menjadi semakin berwarna karena ulah cracker. Mereka akan menjadi anaman bagi para pengharap, pemimpi dan pengangan-angan kebaikan *cyberspace* di samping ancaman dari para pengkritik budaya cyber.

Dari proses kelahiran internet, pemanfaatannya untuk berbagai kegiatan dan harapan-harapan yang digantungkan kepadanya menyebabkan internet telah menjadi kekuatan dan aset dari setiap sisi kehidupan yang memanfaatkannya. Adanya cracker akan mengacau-balaukan harapan-harapan yang telah terlanjur ditanamkan pada internet ini baik oleh pemerintah maupun pengusaha, sehingga mereka menganggap tindakan mereka sebagai suatu kejahatan. Dengan dalih melanggar undang-undang (*seperti Computer Fraud and Abuse Act* di Amerika atau *The Information Technology Act 1999* di India) mereka menangkap dan memenjarakan cracker. Indonesia saat ini juga sedang membuat undang-undang yang hendak menghambat langkah para penjahat cyber ini agar kepentingan-kepentingan yang berkaitan dengan *cyberspace* dapat terlindungi.

Dalam perspektif teori realitas sosial kejahatan, apa yang dilakukan oleh beberapa negara (termasuk Indonesia) dengan mengkategorikan atau menentukan *hacking* sebagai kejahatan merupakan definisi hukum yang diciptakan oleh alat-alat kelas dominan di dalam masyarakat yang secara politis terorganisasi. Tindakan ini dilakukan karena hacking merupakan tindakan atau perilaku yang bertentangan dengan kepentingan kelas dominan. Kelas dominan yang telah menentukan *hacking* sebagai kejahatan adalah pemerintah atau negara dan perusahaan atau pengusaha yang mempunyai kepentingan dan pengharapan yang besar terhadap teknologi informasi. Dengan melihat pada proses-proses yang

telah disebutkan di atas, kepentingan negara atau pemerintah dan pengusaha atau perusahaan terhadap teknologi informasi ini sangat besar. Gangguan terhadap keamanan sebuah atau beberapa situs yang dikelola oleh pemerintah atau pengusaha merupakan hambatan terhadap harapan keuntungan yang akan diperoleh dari penggunaan internet.

Hacking dengan demikian bukanlah kejahatan yang melekat pada perilaku, melainkan lebih merupakan suatu penilaian yang dibuat oleh pihak-pihak terhadap tindakan itu. Penentuan *hacking* sebagai kejahatan merupakan proses dinamika kelas (negara dan pengusaha) yang memuncak dalam penentuan cracker dan perilaku *hacking* sebagai kejahatan. Dengan mendasarkan pada *Declaration of Independence of Cyberspace* dan *Manifesto Hacker*, tindakan *hacking* bukanlah kejahatan karena merupakan perwujudan dari kebebasan untuk mendapatkan informasi. Formulasi kejahatan terhadap *hacking* merupakan manifestasi dari konflik kelas antara pemerintah dan pengusaha (sebagai kelas dominan yang memanfaatkan internet untuk mendapatkan keuntungan) dan para cracker yang mendasarkan diri pada hak asasinya untuk mendapatkan informasi sebagaimana yang tercermin dalam *Declaration of Independence of Cyberspace* dan *Manifesto Hacker*.

Hak untuk mendapatkan informasi dan mengeluarkan pendapat (baik lisan maupun tulisan yang berarti juga informasi untuk orang lain) merupakan hak asasi setiap manusia. Dalam kenyataannya kebebasan ini ternyata tidak berlaku secara luas karena adanya berbagai hambatan yang dikeluarkan oleh pemerintah. Kebebasan memperoleh informasi dan mengeluarkan pendapat di

cyberspace juga tidak sebebas yang diperkirakan sebagaimana pernyataan di bawah ini

> Freedom of speech on network will be promoted by limitating content-based regulations and by promoting competition among providers of network services. The first is necessary because government will be tempteto restrict the content of any information service they subsidize or regulate. The second is necessary because market competition is the most efficient means of ensuring that needs of network users will be met.[76]

Teknologi itu tidak netral, ia dapat dimanfaatkan apa saja untuk keperluan manusia, tetapi teknologi merupakan kekuasaan yang kebesarannya tidak dapat diduga. Manusia yang terpikat sains dan teknologi tanpa disadari ditelan kekuasaan sains dan teknologi sebagai sistem total yang menguasai berbagai bidang kehidupan manusia. Kekuasaan itu sendiri (baik kekuasaan politik maupun eknomi) melestarikan dan memperluas dirinya tidak hanya melalui teknologi melainkan sebagai teknologi, dan teknologi menyediakan legitimasi yang kuat bagi kekuasaan politis yang sedang meluas, yang mengabsorpsi segala bidang kebudayaan.

Cyberspace merupakan hasil dari konstruksi teknologi yang juga telah dipergunakan sebagai alat kekuasaan. Sebagai hasil teknologi, keberadaan cyberspace, apa yang tersaji di dalamnya juga tidak netral, ia dikonstruksi oleh orang-orang yang menginginkan menampilkan apa yang menjadi harapannya. **Thomas E. Miller** seorang pejabat dari *Biara Namgyal* mengatakan "*Cyberspace* merupakan medan yang diciptakan tanpa adanya gangguan. Demikianlah

---

[76] Mitchel Kapor, *op.cit.*

cyberspace dirancang. Ia membangkitkan potensi sesuatu dan sifat yang akan dibangkitkan itu bergantung pada motivasi penggunanya."[77]

Cyberspace adalah dunia simulasi dan karena simulasi tidak menggambarkan realitas sebagaimana adanya, maka realitas yang dihasilkan oleh simulasi adalah realitas yang melampaui. Dalam wacana politik (sebagaiman penggunaan internet untuk kepentingan politik) makna simulasi sebagai penciptaan realitas yang melampaui harus dilihat dalam konteks pendistorsian, pelencengan atau pemalsuan realitas. Dalam sebuah artikelnya yang berani dan brilian, yang menguraikan realitas maya dalam politik Amerika, **Michael Kelly** menegaskan bahwa negara Amerika adalah sebuah Republik Ilusi, negara yang dipimpin bukan oleh para pemimpin hasil pemilu, melainkan oleh orang-orang yang mengemas dan menjual para pemimpin itu kepada rakyat yang semakin mau percaya bahwa (dengan mengutip kata-kata petenis **Andre Agassi**) "*citra adalah segalanya.*" Politik Amerika, menurut *Kelly*, "lebih merupakan realitas maya daripada realitas objektif."[78]

Politik simulasi dalam perspektif teori simbolik interaksionis sangat bergantung pada politik pertandaan atau politik simbol (*politics of signification*) dan politik citra (*politik of image*). Tanda dan citra digunakan sebagai alat untuk memalsukan realitas, untuk membunuh realitas dan kebenaran sehingga kebenaran tersebut terkubur di balik *simulacrum* kebenaran. Logika simulasi adalah *logika pemelintiran* makna (*twisting of meaning*) untuk kepentingan

---

[77] Jeff Zaleski, *op.cit.*, hal. 312

[78] Pernyataan yang menyedihkan ini tidakhanya terbatas pada pusat pemerintahan Amerika di sungai Potomac, tetapi juga mewakili suatu kebudayaan yang "batas antara realitas dengan fantasinya telah musnah, suatu kebudayaan yang telah mengubah Oliver Stone menjadi ahli sejarah dan Barbara Streisand seabgai pemegang otoritas kebijakan nasional." Michael Kelly, *David Gergen, Master of the Game*, New York Times, October 31, 1993. Lihat juga Mark Slouka, op.cit, hal. 133-134

politik atau golongan tertentu, maka ketika media massa menjadi sebuah mesin simulasi, apa yang disajikan kepada masyarakat tak lebih dari rangkaian informasi palsu, rangkaian prostitusi citra, yaitu sebuah citra yang melacurkan kebenaran demi kepentingan politik golongan tertentu.[79]

Untuk menegaskan peran logika simulasi dalam politik, **Paul Virlio** dalam *War and Cinema: The Logistic of Perception* mengatakan bahwa dunia politik modern tidak dapat dilepaskan dari strategi citra dan tontonan serta pemalsuan kebenaran di dalamnya, dengan menciptakan berbagai bentuk tontonan teater untuk publik dalam rangka menciptakan citra yang diinginkan oleh kelompok politik tertentu. Dalam tingkat wacana apa yang dilakukan oleh para tokoh politik dalam memanfaatkan teknologi informasi dapat disebut sebagai wacana *pseudosophy*.

Pseudosophy merupakan sebuah wacana yang berkaitan dengan pencitpaan pengetahuan palsu dan kebenaran semu di dalam masyarakat. *Pseudosophy* menciptakan berbagai bentuk kekerasan simbolik (*symbolic violence*) pada tingkat wacana komunitas politik. Kekerasan tersebut muncul ketika sebuah sistem kekuasaan (atau lembaga kemasyarakatan) menggunakan otoritas kekuasaannya dalam mendefinisikan realitas sesuai dengan selera dan kepentingannya. *Pseudosophy* adalah wacana pseudo-pengetahuan yang melandasi beroperasinya mesin simulasi yang memproduksi berbagai bentuk kepalsuan untuk menciptakan kondisi kekacauan dan konflik di dalam masyarakat.[80]

---

[79] Yasraf, *op.cit.*
[80] *Ibid.*

Penguasa menggunakan teknologi informasi sebagai wacana *pseudosophy* untuk memproduksi kepalsuan-kepalsuan dan di sisi lain penguasa tidak menginginkan pihak lain (lawan politiknya atau siapapun) menggunakan mesin kepalsuan untuk mengganggu aktivitasnya dalam memproduksi kepalsuan. Tindakan yang dilakukan adalah dengan membuat peraturan atau hukum yang melegalkan tindakan penguasa dan membatasi tindakan lawan politiknya.

Meskipun demikian, pemanfaatan teknologi informasi untuk politik juga menjadi inspirasi bagi lawan politiknya atau orang lain (yang memiliki kepentingan pribadi) untuk menggunakan teknologi informasi itu untuk melakukan kejahatan. Berbagai korban telah jatuh, baik di pihak pemerintah yang telah mengelola sebuah atau beberapa situs untuk kepentingan politiknya maupun para pengusaha yang telah menggunakan teknologi informasi untuk keperluan bisnisnya. Kejahatan-kejahatan yang dilakukan dengan menggunakan teknologi informasi ini hampir sebagian besar tidak tertangani dengan baik.

Ketidakberesan dalam menangani masalah kejahatan (dari sentuhan hukum) dengan menggunakan teknologi informasi atau *cybercrime* ini menimbulkan pertanyaan, apakah kejahatan itu yang telah berkembang menjadi begitu sempurna sehingga telah melampaui batas-batas hukum atau sebaliknya apakah perangkat hukum itu sendiri yang telah kehilangan otoritas sehingga tidak kuasa menghadapi kejahatan.

Mayarakat kita tampaknya telah memasuki wacana kejahatan yang melampaui batas realitas (*beyond reality*) sebagaimana yang disinyalir oleh **Jean Baudrillard** dalam *The Perfect Crime*, di mana kejahatan dan kriminalitas telah berkembang sedemikian rupa sehingga mencapai tingkat yang sempurna atau

hiper-kriminalitas (*hyper criminality*). Kejahatan telah menjadi satu wacana yang telah direncanakan, diorganisir dan dikontrol secara sempurna melalui teknologi tinggi (*high technology*), manajemen tinggi (high management) dan politik tinggi (*high politics*) sehingga ia melampaui otoritas hukum, kemampuan akal sehat dan jangkauan nilai-nilai budaya.[81]

Pandangan semacam ini sesuai dengan sifat dari *cyberspace* sebagai dunia yang dihasilkan dari sebuah konstruksi sosial dan teknologi, sebuah dunia yang keberadaannya diinginkan atau dengan kata lain *cybercrime* merupakan kejahatan yang telah dikonstruksikan, telah direncanakan dan diorganisasikan. Sebagai sebuah hasil konstruki, maka di masa mendatang akan ada konstruksi yang lebih sempurna dan ini berarti kejahatan tidak akan habis, ia hanya bisa dilenyapkan sementara. Hal ini terjadi karena kejahatan mudah melakukan regenerasi, metamorfosis atau simbiosis. Ia akan tumbuh lagi pada pohon yang baru dengan wujud yang baru pula. Dari penjelasan tersebut menjadi jelas bahwa penetapan hacking sebagai fenomena cybercrime tidak hanya didasarkan pada kriteria tradisional dalam penentuan kejahatan (berupa kerugian dan reaksi), tetapi ditentukan pula oleh konstruksi sosial yang ada dibaliknya berupa kepentingan politik, sosial, budaya, dan terutama kepentingan bisnis.

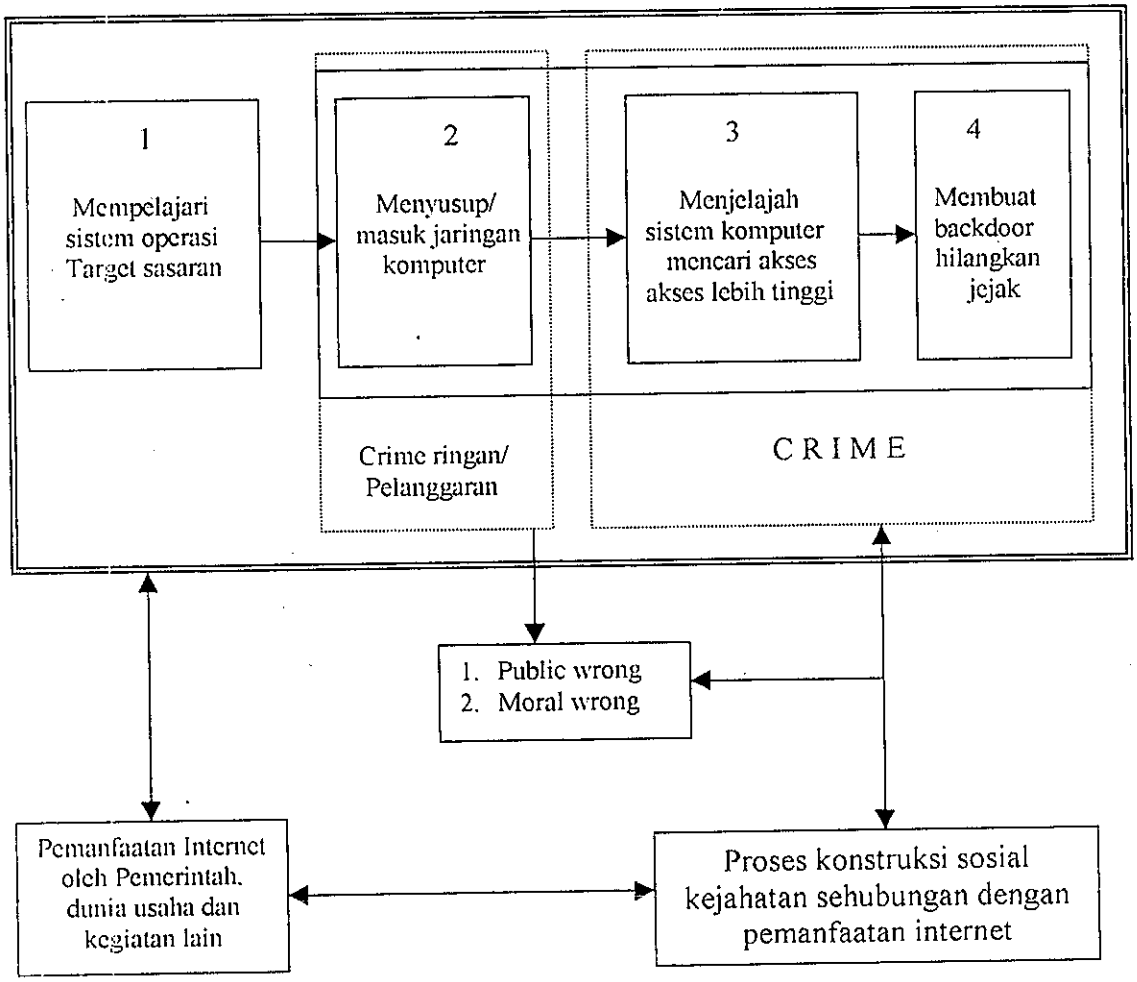
Dari penjelasan di atas secara sederhana dapat diterangkan mengenai tahap-tahap hacking dan konstruksi hacking sebagai kejahatan seperti yang tampak pada bagan 2 berikut ini.

---

[81] Yasraf Amir Piliang, *Hiper Kriminalitas*, Kompas, 30 Oktober 1998, versi elektronik dapat dijumpai di http://www.kompas.com/hipe04.htm

Bagan 2

Konstruksi Kejahatan dari Hacking



B. REAKSI KORBAN *HACKING* DAN ANTISIPASINYA TERHADAP AKTIVITAS *CRACKER* DI KEMUDIAN HARI

1. Korban-korban *Hacking* Di Indonesia

Setiap tindakan akan membawa akibat, demikian pula *hacking*, tindakan yang dilakukan baik oleh *hacker* maupun *cracker* akan menimbulkan korban yang jumlahnya tidak sedikit. Akibat atau timbulnya korban merupakan konsekuensi logis dari sebuah perbuatan. Keberadaannya tidak dapat dihindari

seperti halnya keburukan sebagai pasangan abadi dari kebaikan atau seperti uang yang selalu mempunyai dua sisi yang berbeda.

Keberadaan korban ini tidak dapat dihindari, akan tetapi jumlahnya dapat diminimalisir, jika orang-orang yang terlibat di dalamnya sudah mengetahui resiko yang akan diterima dan mempersiapkan alat pencegah (dalam hal ini adalah sistem keamanan yang diperketat/diperkuat). Kebanyakan korban kurang memperhatikan masalah keamanan ini meskipun mereka menganggap masalah ini sebagai masalah yang penting, bahkan ada yang sama sekali tidak memasang sistem keamanan pada situs yang dikelolanya, seolah-olah mereka percaya bahwa dalam dunia *cyber* ini tidak ada penjahat atau semua *netizen* adalah baik, padahal penjahat dalam jumlah yang besar bergentayangan hampir setiap menit bahkan detik untuk menemukan mangsa yang tepat.

Dengan segala kecerobohan dan kekuranghati-hatian yang ada pada pemilik situs, *webmaster* dan *administrator sistem*, membawa kerugian yang tidak sedikit jumlahnya. Tidak hanya pelayanan situs kepada pengakses yang terganggu, tetapi untuk melakukan *back up* (jika masih ada data yang ada tersedia di lain komputer) memerlukan uang dan waktu yang tidak sedikit. Jika kerusakan yang ditimbulkan oleh serangan *cracker* itu sangat vital seperti hilangnya semua data, *log file* dan matinya semua aplikasi dalam sistem komputer, ini merupakan malapetaka yang menunjukkan betapa cerobohnya pemilik, *webmaster* dan *administrator sistem* dari sistem komputer yang dikelolanya itu.

Cracker dengan aktivitas *hacking*nya mempunyai sejarah yang panjang, tetapi berdasarkan catatan yang dilakukan oleh **Robert H'obbes" Zakon**, seorang *Internet Evangelist*, *hacking* yang dilakukan oleh *cracker* pertama kali dilakukan pada tanggal 12 Juni 1995 terhadap *The Spot* dan tanggal 12 Agustus 1995 terhadap *Crackers Movie Page*.[82] Berdasarkan catatan itu pula, situs pemerintah Indonesia pertama kali mengalami serangan *cracker* pada tahun 1997 sebanyak lima kali, yaitu tanggal 19 Januari, 10 Februari, 24 April, 30 Juni dan 30 November. Pada tahun yang sama, situs *NASA* (5 Maret), *UK Conservative Party* (27 April) dan *Spice Girls* (14 November) juga diserang *cracker*.

Sejak serangan yang pertama itu sampai sekarang, korban-korban serangan *cracker* terus berjatuhan, akan tetapi hampir sebagian besar tidak terpublikasikan sehingga data yang akurat mengenai berapa jumlah yang telah menderita akibat serangan *cracker* tidak dapat dicatat dan dihitung secara pasti. Indonesia, meskipun dapat dikatakan tertinggal dalam mengikuti dan menikamati perkembangan teknologi informasi, juga telah menjadi korban *hacking*. Berikut ini ada beberapa kejadian yang menimpa beberapa situs milik pemerintah dan perusahaan di Indonesia yang telah menjadi korban *cracker* dan dapat diperinci sebagai berikut:

a. Pada tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negeri dan ABRI dijebol oleh *cracker Porto* (Portugis)

---

[82] *Hacking* dalam pengertian ini adalah *hacking* yang dilakukan terhadap situs layanan publik, bukan situs penelitian dan juga bukan situs untuk keperluan pendidikan. Lihat dalam Robert H'obbes' Zakon, *loc.cit.* *Hacking* dalam pengertian yang lebih luas telah mulai ada sejak tahun 1961, ketika Laboratorium kecerdasan di MIT memperoleh sebuah PDP yang kemudian digunakan oleh mahasiswa MIT untuk melakukan penyusupan-penyusupan. Inilah aksi *hacking* yang pertama, sebagai cikal bakal *cracker-cracker* modern.

yang pro kemerdekaan. Disain depan (beranda/*frontpage*) kedua situs tersebut diganti semua. Aksi yang disebut *East Timor Campaign* menambahkan pada situs yang diserang itu dengan kata-kata anti integrasi Timor Timur dan anti ABRI. Dalam tahun yang sama situs pendidikan yang dalam manifesto *hacker* dilarang untuk disentuh, juga dirusak oleh *cracker*. Situs yang menderita tersebut adalah milik LIPI dan Universitas Airlangga. Selain mereka, situs milik harian Media Indonesia juga kena imbas aksi *cracker* Porto itu. Serangan dari *cracker* Porto ini mendapat balasan dari *cracker* Indonesia. Hal ini dilakukan karena menurut mereka *cracker* Porto dinilai keterlaluan, serangannya membabi buta, tidak mempedulikan apakah situs itu milik pemerintah atau bukan, situs bisnis maupun situs pendidikan. *Toxin*, pangkalan Timor Timur di Internet milik kelompok anti integrasi dihancurkan dalam serangan balik. Dari semua serangan balik itu, yang paling menghebohkan adalah serangan balik yang tidak saja menghancurkan *homepage* dan sekaligus menghantam salah satu perusahaan penyedia server di Irlandia yang bernama ***Connect Ireland***, perusahaan yang dikenal sebagai penyedia server untuk situs yang beroperasi di bawah *East Timorese Project* yaitu *web* yang memperjuangkan kemerdekaan Timor Timur dari wilayah Indonesia.

Serangan balik ini terjadi pada akhir tahun 1999. Menurut keterangan yang diberikan oleh administrator *Connect Ireland*, 18 serangan dilakukan secara serempak dari seluruh penjuru dunia. Akan tetapi berdasarkan pengamatan, domain Timor Timur tersebut di*hack* dan kemuian ditambahkan sub domain yang bernama *need.tp*. Berdasarkan pengamatan yang dilakukan oleh **Budi**

Rahardjo, *need.tp* merupakan sebuah perkataan yang sedang dipopulerkan oleh *Beavis and Butthead* (sebuah acara TV di MTV). Dengan kata lain *cracker* yang melakukan serangan tersebut kemungkinan penggemar atau paling tidak pernah menonton acara itu. Jadi kemungkinan dilakukan oleh seseorang dari Amerika Utara.[83]

b. Pada pertengahan tahun 1988, situs milik Pusat Dokumentasi dan Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) yang beralamat di http://www.pdii.lipi.go.id di*hack* oleh orang yang tidak dikenal. Tampilan depan atau frontpage PDII LIPI diganti dengan gambar wanita telanjang. Pengelola situs PDII LIPI tidak bisa mendeteksi siapakah yang melakukan penyerangan dan perusakan terhadap situs yang dikelolanya itu.

c. Tahun 1998, setelah kerusuhan Mei, *cracker* yang berasal dari Cina menghantam situs milik pemerintah. Situs yang tidak beruntung itu adalah situs web milik BKKBN (Badan Koordinasi Keluarga Berencana Nasional) yang diserang oleh *cracker* yang menyebut dirinya ***Discover***. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan. Tidak hanya merusak situs web milik BKKBN, mereka juga mengancam akan merusak situs-situs milik pemerintah Indonesia yang lain.

d. Juni 1999, *cracker* lokal menyerang homepage lokal. Kali ini yang menjadi korban adalah homepage POLRI. *Frontpage* atau gambar depan dari *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip dengan logo atau gambar PDI-P.

---

[83] Budi Rahardjo. *op.cit.* hal. 7.

e. Pada Januari 2000, beberapa situs web Indonesia diacak-acak oleh *cracker* yang menamakan dirinya *fabianclone* dan *naisenodni*. Situs yang diserang antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet. Besarnya kerugian belum bisa dipastikan. Menurut **Hadi Munadi** dari Divisi Komunikasi BEJ, yang diserang oleh para *cracker* itu hanyalah web-nya saja sehingga kerugian yang diderita tidak seberapa dan dapat dipulihkan dalam waktu singkat. Serangan terhadap BEJ ini tidak sampai kepada sistem transaksinya atau lebih dikenal dengan *Jakarta Automatic Trading System* (JATS) karena sampai sekarang transaksi di BEJ belum dapat dilakukan melalui internet (keinginan untuk mengintegrasikan perdagangan lewat internet sampai sekarang belum terwujud). Jika waktu serangan itu terjadi dan sistem perdagangan pada BEJ sudah terintegrasikan ke dalam internet, maka kerugian yang diderita akan lebih besar.[84] Demikian juga dengan BCA, hanya web-nya saja yang diserang dan tidak sampai menyerang sistem transaksi yang telah terintegrasikan ke internet.

f. Pada tanggal 11 Januari 2000, situs penerbitan buku-buku Islam yang beralamat di http://www.mizan.com diserang oleh *cracker* yang menamakan dirinya sebagai Hotmilk@www.com. Akibat serangan itu, seorang yang hendak membuka situs Mizan tidak mendapatkan tampilan yang seharusnya, tetapi akan menjumpai pesan yang disampaikan oleh *cracker* dalam bahasa Inggris. Bunyi pesan tersebut kira-kira sebagai berikut:

> "Maaf, sebetulnya kami hanya mencoba sistem keamanan anda, dan ternyata kami dapati bahwa sistem keamanan anda sangat sangat rapuh.

---

[84] Berdasarkan wawancara dengan Hadi Munadi dari Divisi Komunikasi BEJ pada tanggal 25 Mei 2001 di Ruang Divisi Komunikasi Bursa Efek Jakarta.

> Pembuat sistem keamanan anda (dia menggunakan kata makian) ... suatu hari nanti anda harus berhati-hati, atau sewaktu-waktu kami akan kembali dan melakukan kerusakan lebih dari yang sekarang ini. Jadi tidak usah mencoba mencari tahu siapa saya, cari saya si pembuat sistem keamanan. Ha ... ha... ha ... kami masuk ke server dan website anda tanpa ijin. Hati-hati kawan. Salam dari Hotmilk@www.com."

Haidar Bagir, pemilik Penerbitan Mizan menduga *cracker* yang menyerang situs miliknya berasal dari Australia.[85]

g. September dan Oktober 2000, seorang *cracker* dengan julukan **Fabian Clone** berhasil menjebol web milik Bank Bali. Sebelumnya **Fabian Clone** juga berhasil menjebol web milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking* pada nasabahnya sehingga kerugian yang diderita lebih besar dibandingkan dengan kerugian yang diderita BEJ termasuk terputusnya layanan terhadap nasabah.

h. Pada pertengahan Januari 2001, situs milik PT. Ajinomoto Indonesia diserang *cracker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* yang digunakan sebagai katalis dalam proses pembuatan *monosodium glutamate* (bumbu penyedap rasa) yang mengandung lemak babi. Akibat ulah *cracker* pada situs PT. Ajinomoto yang beralamat di http://www.mjk.ajinomoto.co.id, ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan *tulisan Babi, open in December 2K*. Di samping itu terdapat juga tampilan tulisan yang berwarna-warni yang muncul silih berganti dengan menggunakan bahasa *java* yang jika dirangka akan berbunyi *"Ajinomoto You Lied to Us"*. Di bawah gambar babi tertulis *Ajinomot gift. This little pig went to the Ajinomoto* dan pada bagian judul

---

[85] Republika, 16 Januari 2000, hal. 15.

halaman tersebut terdapat *kalimat "Ajinomoto :: HARAM ... HARAM... HARAM."* Situs ini di*hack* oleh seorang *cracker* yang bernama **boyons** dengan alamat e-mail boyons@crackermail.com.

i. Setelah mendapat serangan pada pertengahan tahun 1998, situs PDII LIPI kembali diserang oleh *cracker* yang sekali lagi tidak dapat diidentifikasi karena tidak meninggalkan jejak. Kerusakan yang ditimbulkan tidak seberapa dibandingkan dengan serangan pertama, karena yang diserang adalah bagian yang disediakan untuk buku tamu dan buku saran/kritik. Bagian tersebut sama sekali hilang dari situs atau dengan kata lain dihapus oleh *cracker*. Serangan ini tidak menyebabkan layanan publik PDII LIPI menjadi terhenti.

j. April 2001, situs web milik Departemen Agama dan Departemen Perindustrian dan Perdagangan dirusak oleh *cracker*. Situs milik Departemen Perindustrian dan Perdagangan tidak sekedar dirusak, tetapi file-file penting dan *log file*-nya dihapus, sehingga administrator sistemnya tidak bisa mendeteksi siapa yang melakukan penyerangan, lagi pula *cracker* tersebut tidak meninggalkan jejak sehingga meyulitkan penelusuran. Untung saja pihak Departemen Perindustrian dan Perdagangan mempunyai *back up* sehingga kerusakan dapat segera diperbaiki.

k. Pada tanggal 8 Mei 2001, situs resmi Kepolisian Republik Indonesia yang beralamat di http://www.polri.go.id. sekitar 10 menit tidak bisa tampil atau tidak dapat diakses karena mendapat serangan dari *cracker* yang menamakan dirinya Kesatuan Aksi *Cracker* Muslimin Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

1. Pada tanggal 25 Mei 2001, situs Riset Unggulan Terpadu (RUT) yang dikelola oleh LIPI dan beralamat di http://www.rut.lipi.go.id diserang oleh *cracker* yang berhasil diidentifikasi. Serangan itu dibuat oleh *sHocking from C.O.S of P.R.C at yeah .... . net.* Serangan ini menyebabkan layanan situs RUT macet total untuk beberapa saat karena data-data penting yang tersedia di situ beserta *log file* dan aplikasinya dihapus oleh *cracker*.

Korban-korban *cracker* yang tersebut di atas adalah korban *cracker* sampai akhir Mei 2001 yang berhasil penulis peroleh. Mengingat perkembangan teknologi informasi yang tiap hari terus berubah dan jumlah *hacker*, *cracker* serta *vandal* komputer semakin bertambah dan ketetutupan korban *hacking* terhadap publikasi atau laporan ke polisi, ada kemungkinan jumlahnya akan bertambah dan terus bertambah. Jumlah korban *cracker* yang telah disebutkan tidak mencerminkan korban *hacking* secara keseluruhan karena banyak korban yang tidak berani mengemukakan atau menyatakan kepada publik bahwa situs yang dikelolanya telah menjadi korban *hacking*.

2. Perpekstif Kriminologis Reaksi Sosial Korban *Hacking*

Menggunakan internet sebagai media untuk berbagai usaha (baik politik, ekonomi, sosial, budaya) merupakan sebuah investasi yang besar. Untuk menyediakan struktur dan infrastruktur jaringan komputer memerlukan dana lebih dari Rp. 100.000.000,-.[86] Dana sebesar itu belum termasuk biaya pemeliharaan dan aktualisasi data yang ditampilkan dalam situs. Untuk dunia

[86] Berdasarkan percakapan dengan Mesnan Silalahi, Pengelola website http://www.rut.lipi.go.id/ dari Sekretariat RUT LIPI pada tanggal 25 Mei 2001.

bisnis, dana sebesar itu sangat diperhitungkan dengan berbagai keuntungan dan kerugian yang mungkin diraih.

Dunia sekarang sedang dilanda apa yang disebut dengan revolusi teknologi informasi. Mereka yang tidak menggunakan internet untuk berbagai kepentingan dikatakan ketinggalan jaman atau buta teknologi. Internet menjadi sebuah gurita dalam kehidupan, sehingga menimbulkan keinginan untuk bergabung di dalamnya. Banyak sebetulnya yang menyadari bahwa bermain di dunia maya ini mengundang resiko yang besar, tidak hanya uang, reputasi bisnis tetapi juga nama baik para *webmaster*.

Mereka yang tergiur dengan janji-janji kemudahan, keuntungan dan juga kelebihan menggunakan internet, berlomba-lomba bermain dalam bidang ini. Uang dalam jumlah besar diinvestasikan dan mereka mendirikan perusahaan yang disebut dengan nama *dot com*. Begitu besarnya investasi dan optimisme yang ditanam sehingga ketika mengalami berbagai kejadian setelah beberapa tahun, mereka menyadari bahwa anggapan mengenai kemudahan, keuntungan dan kelebihan bermain di dunia maya dalam kenyataannya tidak seperti yang dibayangkan, sehingga satu persatu perusahaan *dot com* gulung tikar.

Pemerintah dan institusi lain yang tidak berorientasi bisnis juga mulai melirik internet untuk memberikan pelayanan publik. Dengan dana yang diambilkan dari anggaran negara, instansi pemerintah berlomba-lomba membuka situsnya sehingga hampir semua instansi pemerintah sekarang telah mempunyai situs sendiri. Pada satu sisi, keinginan instansi pemerintah inii baik, artinya mereka ingin memberikan layanan publik dengan baik dan terjangkau oleh siapapun dan di manapun (ingat sifat internet yang lintas waktu dan tempat) tetapi

di sisi lain perlu diperhatikan berapa besar investasi yang telah ditanam, seberapa besar kemanfaatannya bagi rakyat terutama rakyat kecil. Hal ini tentunya perlu dipertimbangkan lagi dengan masak agar tindakan membuka situs tidak dituduh sebagai langkah agar pemerintah tidak dikatakan ketinggalan teknologi atau buta teknologi.

Mengingat investasi yang ditanamkan begitu besar untuk bermain dalam dunia virtual ini, maka ketika mereka mendapat serangan *cracker* atau *cracker* yang menyebabkan kerusakan pada situs yang telah dibangunnya, mereka kalang kabut memperbaikinya. Perbaikan sebuah situs yang telah di*hack* memerlukan waktu yang lama apalagi jika pemilik atau pengelola situs tidak mempunyai *back up* data dan ini berarti harus mulai dari awal lagi, artinya jumlah uang yang dikeluarkan akan semakin besar.

Menanggapi serangan *cracker* yang menimpa situs yang dimilik atau dikelolanya itu, reaksi, tanggapan dan pendapat yang dikeluarkan bermacam-macam suaranya. Pada umumnya para korban sudah tahu resiko bermain di dunia maya, sehingga ketika situsnya di*hack*, para korban menanggapinya dengan nada kesal. "*Mengapa situs kami yang dihack, apakah mereka tidak tahu kalau situs kami ini bukan situs komersial, tetapi situs yang memberikan layanan publik. Jika dihack begini, berapa ratus bahkan berapa ribu pengakses yang tidak bisa kami layani hanya karena ulah seorang cracker atau cracker*," kata beberapa administrator sistem yang dijumpai penulis.[87]

---

[87] Rangkuman pendapat dari berbagai korban yang penulis jumpai seperti Wasi Tri Prasetyo dari PDII LIPI, Mesnan Silalahi dari Sekretariat RUT LIPI, Hadi Munadi dari BEJ dan beberapa pakar dan perumus RUU Teknologi Informasi di Bandung, seperti Budi Rahadjo, Achmad Ramli dan Sigid Suseno.

Pada umumnya reaksi yang diberikan oleh korban *cracker* adalah merasa kaget, kesal dan terakhir mencela ulah *cracker* ini. Akibat ulah *cracker* ini bukan hanya uang yang seharusnya dapat diinvetasikan untuk keperluan lain menjadi terhambat, tetapi keuntungan seperti dijanjikan ketika memasuki *cyberspace* untuk sementara tidak terwujud. Para korban umumnya menganggap serangan *cracker* ini sebagai sebuah kecelakaan, dan mereka tidak mau mempublikasikan atau melaporkan apa yang dideritanya itu kepada polisi meskipun sebenarnya tahu apa yang dilakukan oleh *cracker* itu merupakan tindak kejahatan. Tindakan para korban ini disebabkan oleh beberapa alasan, antara lain.

a. Menanamkan modal atau investasi dengan membuat sebuah situs internet tidak hanya membutuhkan taktik dan strategi bisnis untuk meraih keuntungan, tetapi dananya juga besar. Perkembangan teknologi informasi mengubah paradigma pemasaran konvensional menjadi pemasaran digital dan situs internet menjadi sumber daya yang perlu dilindungi keberadaannya. Jika saingan bisnis (yang juga menggunakan internet sebagai media pemasaran produknya) mengetahui bahwa situs yang dikelola oleh suatu perusahaan yang menyediakan transkasi online rusak karena di*hack* oleh *cracker* atau *bogus hacker*, maka ia akan merasa senang karena lawan bisnisnya telah kecolongan yang menyebabkan keuntungan yang seharusnya diraih hilang atau dialokasikan untuk perbaikan situs itu. Artinya situs perusahaan yang kena *hack* tidak melakukan transaksi pada waktu perbaikan situs yang berarti merupakan peluang bagi lawan bisnisnya untuk mengais keuntungan dari rusaknya situs itu. Perusahaan yang kena *hack* akan berusaha menutupi

kejadian itu agar pelanggannya tidak lari ke lain perusahaan lain untuk mendapatkan barang yang diinginkan.

b. Sebuah situs dibuat oleh seorang *webmaster* atau *web design*. Mereka ahli dalam membuat *website*. Jika situs yang dibuat itu rusak karena serangan *hacker* atau *cracker*, maka bukan hanya perusahaan itu yang mengalami kerugian tetapi juga *webmaster*nya harus bertanggung jawab. Apabila berita mengenai rusaknya situs itu tersebar luas, maka yang dipertanyakan tentunya adalah siapa yang membuat situs itu, sehingga reputasi *webmaster* akan tercemar dengan pemberitaan itu. Intinya pada alasan kedua ini adalah perlindungan terhadap *reputasi webmaster*.

c. *Hacking* merupakan jenis kejahatan yang baru dan tidak semua negara memiliki perangkat hukum dan aparat yang mampu mengantisipasi tindak kejahatan ini termasuk Indonesia. Jika polisi Indonesia belum mampu untuk mengatasi masalah *hacking* untuk apa mereka dilapori, untuk apa kejadian itu diadukan jika tidak ada tindak lanjutnya. Dengan kata lain para korban meragukan kemampuan aparat kepolisian dalam menangani persoalan *hacking*. Kerja polisi dalam hal ini dinilai tidak efektif dan para korban beranggapan lebih efektif ditangani sendiri.

d. Data-data yang ada dalam situs di samping merupakan data yang bersifat publik ada juga data yang bersifat privat. Jika peristiwa *hacking* menimpa sebuah situs perusahaan maupun pemerintah dan dilaporkan polisi, ada kekhawatiran di samping mempertanyakan kemampuan polisi dalam menangani kasus ini, juga kemungkinan polisi melihat data-data privat yang seharusnya tidak boleh dilihat. Inti dari persoalan ini adalah menjaga aspek

kerahasiaan perusahaan yang sepantasnya tidak diketahui oleh orang lain atau orang-orang yang tidak mempunyai kode akses terhadap situs perusahaan atau pemerintah itu.

Tindakan yang dilakukan oleh para korban dengan tidak mau mempublikasikan atau melaporkan kepada polisi ini dalam kriminologi disebut *dark figure*. Ada beberapa faktor menurut **Gabriola Zeviar-Geese**, yaitu:[88]

a. the operational speeds and storage capacity of computer hardware make criminal activity very difficult to detect;
b. law enforcement official often lack the necessary technical expertise to deal with criminal activity in the data processsing environment;
c. many victim of computer crime have failed to create contingency plans to deal with computer crime; and
d. once criminal activity has been detected, many businesses have been reluctant to report criminal activity because of fear of adverse publicity. Loss of goodwill embarrassment, loss of public confidence, investor loss, or economic repercussions.

Seperti disebutkan di atas, reaksi terhadap ulah *cracker* ini bermacam-macam. Pada umumnya mereka menganggap bahwa ulah *cracker* ini merugikan bahkan ada yang berpendapat *hacking* merupakan perbuatan amoral.[89] Para korban yang berhasil ditemui menganggap apa yang dilakukan *cracker* sebagai tindak pidana. Meskipun di antara para korban ada yang menganggap ulah *cracker* itu sebagai keisengan belaka, akan tetapi keisengan yang menimbulkan malapetaka. Para korban menganggap atau memberi stigma bahwa *cracker* adalah penjahat.

Sebenarnya tidak hanya para korban *hacking* yang menganggap tindakan *cracker* sebagai kejahatan, berdasarkan etika *hacker* yang dikemukakan oleh **Steven Levy** dan **Lyod Blankeaship**, *hacking* juga tidak diperbolehkan. Artinya

---

[88] Bagriola Zeviar-Geese. *The State of the Law on Cyberjurisdiction and Cybercrime on the Internet*, versi elektronik dapat dijumpai di http://www.law.gonzaga.edu/border... yberlaw.htm

[89] Wawancara dengan Mesnan Silalahi dari Sekretariat RUT LIPI tanggal 28 Mei 2001.

para penghuni *cyberspace* atau *netizen* juga tidak setuju dengan ulah *cracker* yang dianggapnya sebagai perilaku menyimpang, tidak hanya menyimpang dari etika *cracker* yang telah digariskan, akan tetapi juga melanggar hak-hak yang telah digariskan dalam *The Declaration of the Rights of Netizens* yang disusun oleh **Ronda Hauben**. Stereotip jahat yang disandang oleh *cracker* akan terus melekat selama ia melakukan aksinya, bahkan sampai ia ditangkap oleh polisi dan dihukum. Stereotip jahat akan tetap melekat sampai ia keluar dari penjara kecuali mereka-mereka yang beruntung mendapatkan pekerjaan yang baik karena keahlian *hacking*nya itu.

Dalam perspektif kriminologi, penilaian negatif terhadap cracker merupakan akibat dari penilaian sosial dari para korban, *netizen* dan juga masyarakat pada umumnya yang mengetahui kemanfaatan menggunakan internet. Seperti dikatakan oleh **Howard Becker** yang melihat kejahatan tergantung dari penglihatan si pengamat yang melihat anggota kelompok memiliki pandangan yang berbeda konsep tentang apa yang baik dalam situasi terntu, maka dengan mendasarkan pada pendapat **I.S. Susanto,**[90] peranan masyarakat luas dalam mengidentifikasikan atau memproses kejahatan perlu mendapat perhatian yang lebih dibandingkan dengan profil atau pribadi penjahat yang sebelumnya telah mendapat perhatian yang berlebih dalam pembahasan teori-toeri kriminologi pada dekade sebelumnya. Langkah selanjutnya adalah meningkatnya perhatian dan studi terhadap bekerjanya aparat penegak hukum pada umumnya dan khususnya polisi (dan aparat penegak hukum lainnya khususnya dalam menangani kegiatan *hacking*).

---

[90] I.S. Susanto. Kriminologi. FH UNDIP Semarang. 1995. hal. 76.

Penjelasan mengenai kejahatan dalam hubungannya dengan sikap masyarakat dapat diperoleh dengan manganalisa reaksi-reaksi masyarakat yang langsung dialami oleh pelaku kejahatan. Inilah yang dinamakan **oleh Ian Taylor, Paul Walton** dan **Jock Young** *sebagai a social psychology of social reaction.* Reaksi sosial masyarakat yang diberikan kepada penjahat dan kejahatanya berkaitan dengan latar belakang ekonomi, sosial dan politik yang melandasi bekerjanya reaksi sosial yang resmi maupun dari masyarakat untuk mengendalikan tingkat kejahatan di lingkungannya.

Masyarakat, dalam hal ini *netizen* dan orang-orang yang dapat melihat kemanfaatan internet, sebelum memberikan reaksi terhadap tindakan *hacking* sebelumnya sudah mempunyai pandangan yang tercipta sebagai rangkaian proses konstruksi. Proses konstruksi ini terjadi dengan berbagai cara, dalam pendidikan, pergaulan maupun dengan pengamatan terhadap kehidupan sehari-hari disekitarnya. Dalam perspektif para konstruksionalis, pendidikan, pergaulan dan pengamatan merupakan proses pembentukan konstruksi pikiran, pemahaman, pengetahuan dan keterampilan mengenai apa yang dipelajarinya. Pengetahuan itu bukanlah suatu fakta yang tinggal ditemukan, melainkan suatu permusan yang diciptakan orang yang sedang mempelajarinya. Pengetahuan itu suatu konstruksi orang yang sedang mengetahui. Pengetahuan itu (mengandung) suatu proses, bukan fakta yang statis. Dalam arti ini, pengetahuan itu tidak pernah lepas dari orang yang sedang mengetahui.[91]

Secara ringkas gagasan konstruktivisme mengenai pengetahuan dapat dirangkum sebagai berikut:[92]

---

[91] Paul Suparno, *Filsafat Konstruktivisme Dalam Pendidikan*, Kanisius, Yogyakarta, 2001, hal. 14.
[92] Ringkasan dari pendapat von Glasersfeld dan Kitchener, 1987 oleh Paul Suparno, *Ibid*, hal. 21

a. Pengetahuan bukanlah merupakan gambaran dunia kenyataan belaka, tetapi selalu merupakan konstruksi kenyataan melalui kegiatan subjek.
b. Subjek membentuk skema kognitif, kategori, konsep dan struktur yang perlu untuk pengetahuan.
c. Pengetahuan dibentuk dalam struktur konsepsi seseorang. Struktur konsepsi membentuk pengetahuan bila konsepsi itu berlaku dalam berhadapan dengan pengalaman-pengalaman seseorang.

Seseorang yang memperoleh pengetahuan baru tidak serta merta dapat mengubah pandangan atau pendapat tentang sesuatu karena manusia sebelumnya telah menerima pengetahuan sebagai sebuah konstruksi yang telah tertanam dalam pikiran. Dengan demikian ada batasan-batasan yang membatasi konstruksi pengetahuan. **Bettencourt** menyebut beberapa hal yang dapat membatasi proses konstruksi pengetahuan manusia, yaitu konstruksi kita yang lama, domain pengalaman kita dan jaringan struktur kognitif kita. Hasil dan proses konstruksi pengalaman kita yang lampau dapat menjadi pembatas sekaligus mempengaruhi pembnetukan konstruksi pengetahuan kita di masa mendatang.[93]

Hasil konstruksi ini memberikan warna atau pengetahuan yang terlihat dari sikap atau perilaku dan pendapat yang dikemukakan terhadap suatu perbuatan. Bagi *netizen* dan orang-orang yang dapat melihat kemanfaatan, hasil dari proses konstruksi ini terlihat dalam reaksi mereka terhadap ulah *cracker* yang menimbulkan kerugian dan melanggar kepentingan umum maupun privat.

Dalam konteks orientasi teori labeling, *cracker* dipandang sebagai orang yang terpisah dari *netizen* yang terdiri dari orang-orang yang jujur dan patuh yang

---

[93] *Ibid.* hal. 22

menjunjung deklarasi hak asasi *netizen* dan etika *hacker* (atau karena ketidakmampuannya melakukan *hacking*). *Cracker* merupakan penyakit di kalangan *netizen*, sebagai hasil dari berbagai ciri khusus individu baik biologi maupun sosialnya sehingga harus dijauhi dalam pergaulan *netizen*. Tetapi perlu diingat bahwa mereka mempunyai dan membentuk sub kulturnya sendiri di kalangan *cracker*. Di antara mereka telah terjalin komunikasi yang berlangsung terus secara kontinue meskipun komunikasi itu hanya melalui bit-bit yang menyusuri infrasturktur telekomunikasi. Mereka merupakan kelompok ekslusif, terasing dari pergaulan *netizen* yang berperilaku baik dan memerlukan persyaratan tertentu untuk menjadi anggotanya.

Berbeda dengan pendapat **Frank Tannembaum** yang memandang kejahatan merupakan hasil dari ketidakmampuan seseorang untuk menyesuaikan diri dengan kelompok,[94] maka dalam kasus *hacking* ini, *cracker* bukan tidak dapat menyesuaikan diri dengan kelompok atau masyarakat (*netizen*), akan tetapi dalam hal ini *cracker* betul-betul mampu menyesuaikan diri dengan masyarakat yang terbukti mampu berkomunikasi dengan *netizen* lain baik melalui *e-mail, chatting* maupun membuka *web* sendiri. Menjadi *cracker* bukan merupakan kegagalan menyesuaikan diri dengan *netizen*, tetapi merupakan usaha untuk menyesuaikan diri dengan kelompok *cracker* dengan kemampuan yang dimilikinya karena tidak semua *netizen* mampu menjadi *cracker*. Jadi dalam hal ini menjadi *cracker* merupakan karier, yang dilalui dengan berbagai tahap pembelajaran dan kelompok *cracker* tidak begitu saja menerima seseorang untuk menjadi anggotanya (dan tidak ada paksaan untuk itu) tanpa melalui proses

---

[94] Lihat dalam Romli Atmasasmita. *op.cit*. hal. 38

seleksi seperti yang telah disebutkan dalam prinsip dan budaya *cracker*. Dalam hal ini kejahatan merupakan hasil konflik antara kelompok *cracker* (minoritas) dengan *netizen* (mayoritas), di mana terdapat dua definisi yang bertentangan mengenai tingkah laku yang layak.

Dalam konteks teori labeling, *cracker* dipandang bukan sebagai orang yang jahat atau salah perilakunya tetapi sebagai individu yang oleh sistem peradilan pidana dan sebagaian besar masyarakat ditempatkan sebagai orang yang mempunyai status jahat.[95] Fokus teori labeling pada reaksi orang lain dan berikutnya efek reaksi dari perbuatan yang dilakukan oleh penyimpang (*deviance*). Ketika reaksi itu menjadi pengetahuan bahwa seseorang telah melakukan perbuatan menyimpang, si penyimpang kemudian dipisahkan dari masyarakat dan diberi label sebagai penjahat. Inilah yang oleh **Becker** dinamakan ***outsiders***, orang yang diusir atau terusir dan diasingkan dari masyarakat. Orang-orang yang disebut *outsiders* itu kemudian mulai membentuk asosiasi atau perkumpulan dengan orang lain yang juga menjadi orang yang diusir/buangan seperti ***Legion of Doom***, ***Legion of Crackers, 414 Gang*** (kelompok *cracker* remaja di Milwaukee yang berhasil membobol sistem Los Alamos National Lab dan instansi pemerintah Amerika Serikat pada tahun 1982), ***Inner Circle, Master of Deception*** dan lain-lain.

Cap atau label yang diberikan kepada *cracker* akan berpengaruh terhadap *cracker* tersebut, bukan saja pada tingkah laku dalam pergaulan masyarakat di dunia nyata dan dunia maya, tetapi juga usaha-usahanya untuk

---

[95] Hal ini sesuai dengan apa yang dikemukakan oleh Howard Becker, "Deviance is not a quality of the act the person commits, but rather a consequence of the application by others of rules and sanctions to an offender. The deviant is one to whom that label has successfully been applied; deviant behavior is behavior that people so label." Howard Becker, *loc.cit.*

memperbaiki perilakunya. Kesulitan untuk memperoleh dukungan dari masyarakat dalam memperbaiki perilakunya dan kewaspadaan masyarakat terhadap tingkah laku penyimpang atau penyimpang itu semakin memperkuat penyimpang untuk membentuk karir kriminalnya semakin kuat, sehingga tidak mengherankan para *cracker* tidak hanya sekali atau dua kali melakukan *hacking*, bahkan berkali-kali seperti yang dilakukan oleh **Kevin Mitnick, Kevin Poulsen** dan *cracker* lain yang masuk dalam ***Hacker Hall of Fame.***

Ketidakmampuan polisi dalam menangani aktivitas *hacking* juga menjadi sorotan dari para korban *cracker*. Ketidakmampuan ini telah mengubah paradigma teori labeling yang mengasumsikan tindakan penangkapan merupakan proses awal dari labeling. Polisi belum dapat menangkap *cracker* yang meng*hack* sebuah situs (termasuk ketidakmampuan menangkap *cracker* yang menyerang situs Polri sendiri) sehingga langkah awal dari proses labeling berupa penangkapan tidak ada. Proses awal dari labeling justru terdapat dari laporan-laporan media massa yang secara gencar memberitahukan aktivitas *hacking*.[96]

Menjadi *cracker* merupakan suatu proses dan karier tersendiri. Ketika seorang *cracker* melakukan *hacking* untuk pertama kali, maka ia akan tertantang untuk melakukan *hacking* berikutnya agar bisa masuk dan diakui sebagai anggota kelompok *cracker*. Artinya *hacking* pertama memberikan harapan bahwa ia akan menjadi bagian dari kelompok ekslusif dalam *netizen*. Ini merupakan penjungkirbalikan dari pendapat **Lemert** yang menyatakan *primary*

---

[96] Bandingkan dengan pendapat Schrag pada point lima yang mengungkapkan penangkapan sebagai proses awal labeling. Schrag sebagaimana dikutip oleh Romli Atmasasmita, *op.cit*, hal. 39-40

deviance tidak berarti bagi kepribadian pelaku.[97] *Hacking* pertama sangat berarti bagi *cracker* dan ini merupakan pertanda untuk melakukan penjelajahan lebih lanjut.

Cracker yang telah lama berkecimpung dan telah mendapat cap atau label jahat memang sulit untuk melepaskan label jahat itu, artinya setiap tindakannya selalu diidentikkan dengan kejahatannya. Dalam hal ini kejahatan dapat dipandang sebagai karier atau dalam pandangan **Lemert** merupakan *secondary deviance*. Sangat sulit untuk melepaskan cap atau label jahat yang terlanjur telah melekat pada diri seorang *cracker*, tetapi bagi *cracker* cap itu bukanlah akhir dari karier dalam urusan *hack* meng*hack*. Kadang-kadang menjadi *cracker* merupakan berkah karena di samping aspek negatif yang diterimanya (cap sebagai penjahat) maka ada dampak positifnya, yaitu mendapatkan pekerjaan untuk pengembangan software atau diberbantukan pada lembaga kepolisian untuk membantu penyelidikan kasus-kasus *hacking* seperti yang terjadi di India. Jadi *secondary deviance* tidak berhenti pada cap jahat yang melekat sepanjang hidup tetapi karier itu dapat juga melenceng dan menjadi orang baik-baik bahkan menjadi alat untuk menumpas *hacking* yang dilakukan oleh *cracker* lain.

Dengan tidak mengurangi rasa hormat pada pada kritikus teori labeling, pembahasan mengenai stigma atau cap jahat pada *cracker* memang tidak bertalian secara erat dengan aspek personal penjahat sebagai suatu interpretasi yang didasarkan pada kriminologi positif. Menjadi *cracker* bukanlah faktor keturunan dan tidak dapat ditentukan lewat ciri-ciri fisik yang menjadi faktor

---

[97] I.S. Susanto, op.cit, hal. 77, lihat juga Romli Atmasasmita, op.cit, hal. 40

bawaan sejak lahir. Untuk menjadi *cracker* atau menyandang sebutan *cracker* memerlukan proses pembelajaran. Orang yang mempunyai ciri-ciri fisik seperti seorang penjahat tidak dapat serta merta dapat menjadi seorang *cracker*. Penggolongan *cracker* menjadi seorang penjahat hanya dapat dilakukan oleh orang-orang yang merasakan aktivitas *cracker* (*hacking*) dan orang-orang yang melihat kemanfaatan yang diberikan internet. Orang-orang yang tidak tahu apa itu internet dan kemanfaatannya tentu tidak akan menganggap penting hal ini. Reaksi yang ditimbulkan oleh masyarakat merupakan konstruksi sosial politis yang dilakukan oleh masyarakat pengguna internet dan bukan konstruksi psikologis.

Jika teori labeling menaruh perhatian pada rakyat lapisan bawah, golongan minoritas dan sejenisnya sehingga yang dipersoalkan adalah persoalan tentang kekuasaan yang diperoleh oleh mereka yang berkuasa yang menggunakan kekuasaanya untuk menekan kaum yang lemah, maka pendirian ini tampaknya perlu didekonstruksi. Para pelaku *hacking* biasanya bukan dari kalangan lapisan bawah, mereka memang minoritas dibandingkan dengan seluruh masyarakat pada umumnya, tetapi mereka bukan termasuk lapisan bawah.

Pada umumnya mereka adalah kaum terpelajar, setidak-tidaknya pernah mengenyam pendidikan formal sampai tingkat tertentu dan dapat menggunakan atau mengoperasikan komputer. Orang-orang yang termasuk lapisan bawah, khususnya di Indonesia (dan karena kemampuannya biasanya hanya melakukan kejahatan konvensional) pada umumnya tidak bisa menggunakan atau mengoperasikan komputer bahkan buta dengan teknologi informasi sehingga asumsi dari teori labeling yang menaruh perhatian pada rakyat lapisan bawah ini

sekali lagi perlu didekonstruksi. Para *cracker* adalah orang yang berpendidikan, tidak buta teknologi, secara ekonomis mampu dan tidak termasuk dalam masyarakat lapisan bawah.

Pelaku *cybercrime* sebenarnya dapat diklasifikasikan sebagai *white collar crime* dengan menggunakan kriteria yang dipakai oleh **JoAnn L. Miller**. **JoAnn L. Miler** membagi kategori *white collar crime* menjadi 4 (empat), yaitu:[98]

a. Organizational occupational crime

Kategori pertama ini dapat disebut sebagai kejahatan korporasi (corporate crime). Para pelakunya adalah para eksekutif yang dalam hal ini melakukan perbuatan ilegal atau merugikan orang lain demi kepentingan atau keuntungan korporasi.

b. Government occupational crime

White collar crime jenis ini pelakunya adalah para pejabat atau birokrat yang melakukan kejahatan untuk kepentingan dan atas persetujuan atau perintah negara atau pemerintah

c. Professional occupational crime

Jenis ketiga dari white collar crime ini untuk beberapa hal dapat disebut sebagai malpraktek (*malpractice*). Kalangan dokter, psikiater, ahli hukum, pialang, akuntan, penilai (*adjuster*) dan berbagai profesi lainnya yang memiliki kode etik khusus adalah mereka yang melakukan kesalahan

---

[98] JoAnn L. Miller, *White Collar Crime*, Jurnal Ilmu-Ilmu Sosial 5 (Kejahatan Kerah Putih), PAU IS UI dan PT. Gramedia Pustaka Utama, Jakarta, Januari 1994, hal. 31. Lihat juga Johannes Sutoyo dan Adrianus Meliala, *Politik Kejahatan TerhadapPelaku White Collar Crime*, Jurnal Ilmu-Ilmu Sosial 5, PAU IS UI dan PT. Gramedia Pustaka Utama, Jakarta, Januari 1994, hal. 10. Bandingkan dengan Barda Nawawi Arief yang menyatakan cybercrime sebagai dimensi baru dari white collar crime. Barda Nawawi Arief, *Antisipasi Penanggulangan Cyber Crime Dengan Hukum Pidana*, Makalah pada Seminar Nasional Cyberlaw, diselenggarakan STH Bandung, 9 April 2001, hal. 1.

profesional disengaja (*tort*) dapat dikategorikan sebagai professional occipational crimer.

d. Individual occupational crime

Jenis keempat ini ditujukan kepada perilaku menyimpang yang dilakukan oleh para pengusaha, pemilik modal atau orang-orang yang independen lainnya, walaupun mungkin tidak tinggi sosial ekonominya tetapi berjiwa petualang. Dalam bidang kerjanya, kalangan ini kemudian memilih jalan menyimpang yang melanggar hukum atau merugikan orang lain. Sebagai contoh pedagang yang menipu pembeli atau warganegara yang melakukan *tax fraud*.

Cracker adalah orang yang secara teknis memiliki pengetahuan atau mendapatkan pendidikan tentang komputer. Mereka ahli menggunakan atau memainkan jari-jari di atas *keyboard* komputer sehingga kriteria profesional bisa diterapkan kepadanya. Kemampuan mereka menggunakan komputer dapat digunakan untuk melakukan kejahatan dan mereka tentunya memilih korban sesuai dengan kemampuan hackingnya (terutama pada target yang menggunakan sistem operasi komputer yang bahasa pemrogramannya dikuasai).

Sebagai sebuah *white collar crime*, ia juga memenuhi kriteria lain sebagaimana dikatakan oleh **J.E. Sahetapy. Sahetapy** mengatakan

> "white collar crime dapat dipandang ibarat alkohol, makin lama diteguk makin hilang wawasan dan kontrol terhadap diri, sehingga yang bersangkutan menjadi alkoholik. Sekali sampai alkoholik, tidak mudah untuk mengawasi, mencegah apalagi memberantasnya. Jika ia berbaur dan memperoleh sahabat karib dalam dunia kekuasaan (dalam cyberspace, pen) dan ikut menyerap aspirasi terselubung dengan asoirasi politik dalam penampilannya ke luar, maka ia akan sulit dikekang dengan segala akibat serta dampak terhadap masyarakat, bangsa dan negara."[99]

---

[99] J.E. Sahetapy, *White Collar Crime, Sebuah Perspektif Viktimologi*, Jurnal Ilmu-Ilmu Sosial 5 (Kejahatan Kerah Putih), PAU IS UI dan PT. Gramedia Pustaka Utama, Jakarta, Januari 1994, hal. 3

Menjadi seorang *cracker* seperti seorang alkoholik. Begitu ia dapat meng*hack* sebuah situs, maka ia akan tertantang untuk meng*hack* situs yang lain sampai ia mendapat pengakuan sebagai seorang *hacker* atau *cracker* baik dari kalangan *hacker* atau *cracker* itu sendiri. Jadi kriteria *primary deviance* tidak berlaku untuk para alkoholik termasuk cracker sebagaimana disebutkan di atas.

3. Antisipasi Korban *Hacking* Terhadap Aktivitas *Cracker* Di Masa Mendatang

Melindungi aset yang telah ditanamkan, apalagi aset itu akan atau telah memberikan kontribusi terhadap keuntungan yang diperoleh perusahaan atau pemerintah, sangat penting. Perlindungan terhadap aset-aset yang dipakai untuk bermain dalam dunia *cyberspace* ini seharusnya merupakan prioritas utama sebab dalam dunia maya tidak ada jaminan keamanan. Data, informasi dan berbagai hal yang berharga lalu lalang dalam sebuah lalu lintas *superhighway* tanpa pengawasan dari pihak keamanan padahal penjahat dengan mata yang tajam berusahan menghentikan atau mengintersepsi data atau informasi yang berharga itu. Sehubungan dengan tidak adanya pengawasan dalam lalu lintas *superhighway* itu maka masalah keamanan tentunya menjadi tanggung jawab dari mereka yang sengaja menggunakan internet untuk berbagai keperluan.

Mengingat masalah keamanan ini sangat penting, maka sistem keamanan internet itu sendiri merupakan aset yang berharga.[100] Seberharganya aset ini dapat dilihat dari fungsinya sebagai benteng pertahanan ataupun sebagai

---

[100] Keamanan sistem informasi berbasis internet merupakan bagian yang sangat penting dalam internet seiring dengan berkembangnya fungsi keamanan pada komunitas utama sektor komersial dan berbagai aplikasi lain yang dianggap semakin penting. Dalam dunia bisnis (baik bisnis informasi maupun bisnis lain yang menggunakan internet), perkembangan teknologi sistem keamanan ini meningkat dengan pesat dan bisa diterapkan pada berbagai platform teknologi e-commerce yang berbeda-beda, khususnya untuk melengkapi sistem secure digital payment. Intinya sistem keamanan menjadi bagian yang sangat penting dari transaksi-transaksi yang terjadi. Intinya, sistem keamanan informasi adalah power. Onno W. Purbo dan Aang Arif Wahyudi, *Mengenal eCommerce*, Elex Media Komputindo, Jakarta, 2001, hal. 13

pelindung dari berbagai data penting baik yang terdapat di ruang publik maupun ruang privat sebuah situs. Meskipun masalah keamanan ini sangat penting dalam dunia cyberspace, tetapi ada saja yang tidak memperhatikan atau kurang perhatian terhadap sistem keamanan internet yang digunakan pada sebuah situs yang dikelolanya.

Kurang perhatian terhadap masalah keamanan internet ini menyebabkan situs yang dikelola dapat dengan mudah diserang, disusupi, dirusak dan diberi virus yang berbahaya. Dari hasil survey yang dilakukan oleh peneliti pada beberapa korban aksi *cracker*, ternyata responden yang ditemui peneliti menganggap masalah keamanan ini penting tetapi belum menjadi perhatian utama. Meskipun mereka memandang masalah ini penting, tetapi dalam kenyataannya situs mereka berhasil di*hack*, dengan kata lain apa yang diungkapkan oleh mereka mengenai sistem keamanan internet sebagai masalah yang sangat penting baru sebatas perhatian dalam bentuk kata-kata. Ada beberapa hal yang menyebabkan situs mereka berhasil di*hack*, yaitu:

a. Kurangnya perhatian terhadap ungkapan yang menyatakan bahwa dalam dunia internet tidak ada jaminan keamanan yang menyebabkan mereka kurang memperhatikan masalah keamanan. Hal ini dapat timbul karena ada anggapan bahwa pengakses adalah orang baik-baik, orang yang hanya mencari informasi tanpa merusak situs yang dikunjungi. Sebuah anggapan yang keliru dan salah besar. Anggapan ini umumnya muncul dari pengelola situs pelayanan publik milik pemerintah.
b. Berdasarkan anggapan itu maka mereka membangun sistem keamanan internet secara sederhana, murah dan mudah didapat. Sistem keamanan internet yang mereka bangun umumnya berbasis *password*, sebuah sistem keamanan yang sebetulnya sangat rapuh dan mudah ditembus apalagi dengan

adanya berbagai macam aplikasi pemecah password seperti *crack* (UNIX), *viper* (perl script) dan *cracker jack* (DOS).

c. Untuk membangun sistem keamanan internet yang baik memerlukan biaya yang besar, akibatnya mereka beranggapan keamanan internet penting, tetapi untuk memakai sistem keamanan yang mahal (dan tentunya handal) nanti dulu. Jika situs yang dikelola bisa diamankan dengan sistem keamanan yang murah, mengapa harus pakai yang mahal.

Anggapan-anggapan ini melekat pada pengelola situs dan mereka baru menyadari keadaan dan pentingnya keamanan internet jika sudah kena *hack*. Pemikiran untuk menggunakan sistem keamanan yang baik muncul setelah situsnya kena hack. Bagi mereka (terutama situs-situs komersial yang mampu secara finansial) kemahalan bukan halangan untuk melindungi aset yang berharga yang nantinya akan memberikan keuntungan pada era teknologi informasi ini. Bagi situs-situs yang pengembangannya tergantung pada anggaran negara tentunya membangun sistem keamanan yang mahal menjadi suatu kendala sendiri, sehingga para pengelola situs itu mempergunakan cara alternatif yang kemungkinan bisa dimanfaatkan.

Pada umumnya pengamanan sebuah situs dapat dikategorikan menjadi dua jenis, yaitu pencegahan (*preventif*) dan pengobatan (*recovery*). Usaha pencegahan dilakukan agar sistem informasi tidak memiliki lubang keamanan. Hal ini dapat dilakukan pada waktu membangun situs untuk pertama kali ataupun pada waktu situs telah beroperasi tetapi belum pernah di*hack*. Sementara usaha-

usaha pengobatan dilakukan apabila lubang keamanan sudah dieksploitasi atau situs sudah di*hack*.[101]

Ada beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet yang telah dibangun, yaitu:[102]

a. Mengatur akses (*access control*)

Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatus akses ke informasi melalui mekanisme *authentication* dan *access control*. Implementasi dari mekanisme ini antara lain dengan menggunakan password. Di sistem UNIX dan Windows NT, untuk masuk dan menggunakan sistem komputer, pemakai harus melalui proses authentication dengan menuliskan *userid* (*user identification*) dan *password*. Apabila keduanya valid maka pemakai diperbolehkan untuk masuk dan menggunakan sistem tetapi apabila diantara keduanya atau salah satunya tidak valid maka akses akan ditolak. Penolakan ini tercatat dalam berkas log berupa waktu dan tanggal akses, asal hubungan (*connection*) dan berapa kali koneksi yang gagal itu.

Setelah proses *authentication*, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *access control*. *Access control* ini biasanya dilakukan dengan mengelompokkan pemakai dalam sebuah group seperti gorup yang berstatus pemakai biasa, tamu dan ada pula administrator atau disebut juga *superuser* yang memiliki kemampuan lebih dari group lainnya.

---

[101] Budi Rahardjo, *op.cit*, hal. 51. Bandingkan dengan pendapat Arianto Mukti Wibowo yang terdapat dalam makalahnya berjudul Keamanan Dalam Teknologi Informasi, makalah pada seminar Nasional RUU Teknologi Informasi, Gradhika Bakti Praja, Semarang, 26 Juli 2001.

[102] *Ibid*, hal. 52-64 dan berdasarkan wawancara dengan Budi Rahardjo pada tanggal 30 Mei 2001 di PAUME ITB Bandung.

Pengelompokan ini disesuaikan dengan kebutuhan dari penggunaan sistem yang ada.

b. Menutup *service* yang tidak digunakan

Seringkali dalam sebuah sistem (perangkat keras dan/atau perangkat lunak) diberikan beberapa servis yang dijalankan sebagai *default*, seperti pada sistem UNIX yang sering dipasang dari vendornya adalah *finger, telnet, ftp, smtp, pop, echo* dan sebagainya. Dalam praktek pengelolaan situs, tidak semua servis itu dipakai/dibutuhkan sehingga untuk mengamankan sistem service yang tidak diperlukan di server (komputer) tersebut sebaiknya dimatikan. Hal ini dilakukan karena banyak kasus terjadi yang menunjukkan abuse dari servis tersebut, atau ada lubang keamanan dalam servis tersebut akan tetapi administrator sistem tidak menyadari bahwa servis tersebut dijalankan di komputernya.

c. Memasang proteksi

Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa *filter* (secara umum) dan yang lebih spesifik adalah *firewall*. Filter dapat digunakan untuk memfilter e-mail, informasi, akses atau bahkan dalam level packet. Sebagai contoh di sistem UNIX ada paket program *tcpwrapper* yang dapat digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya servis untuk telnet dapat dibatasi untuk sistem yang memiliki nomor IP tertentu atau memiliki domain tertentu. Sementara *firewall* digunakan untuk melakukan filter secara umum. Ada juga program filter internet yang bernama *ZeekSafe*. Program ini bisa memblokir situs-situs yang tidak diinginkan selama pengguna (terutama anak-anak) serfing di internet. Program filter ini sangat membantu bagi pengguna yang was-was terhadap pengaruh buruk internet terhadap anak-anak.

Selain itu ada juga program filter yang lain yaitu *We-Blocker*. Sama dengan *ZeekSafe*, program ini bisa menentukan parameter apa saja yang akan membatasi akses ke website yang dianggap tidak layak dilihat. Tujuh kategori seperti pornografi, kekerasan/kriminal, narkoba/alkohol, perjudian, perselisihan ataupun yang berhubungan dengan senjata tajam adalah contoh situs yang dapat diblokir dengan progam filter ini. Program filter ini dapat diperoleh secara gratis di internet.

d. Firewall

Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini. Tujuan utama dari firewall adalah untuk menjaga (*prevent*) agar akses (ke dalam maupun keluar) dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan. Konfigurasi dari firewall berganting kepada kebijaksanaan (*policy*) dari organisasi yang bersangkutan, yang dapat dibagi menjadi dua jenis, yaitu

1) apa-apa yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (*prohobitted*); dan
2) apa-apa yang tidak dilarang secara eksplisit dengan diperbolehkan (*permitted*).

Firewall bekerja dengan mengamati paket IP (*Internet Protocol*) yang melewatinya. Berdasarkan konfigurasi dari *firewall* maka akses dapat diatur berdasarkan *IP address, port* dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing *firewall*.

Firewall dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu sehingga pamakai (administrator) tinggal melakukan konfigurasi dari firewall tersebut. Firewall juga dapat berupa perangkat lunak

yang ditambahkan pada sebuah server (baik UNIX maupun Windows NT) yang dikonfigurasikan menjadi firewall. Firewall biasanya melakukan dua fungsi, yaitu fungsi *(IP) filtering* dan fungsi *proxy*. Keduanya dapat dilakukan pada sebuah perangkat komputer (*device*) atau dilakukan secara terpisah. Beberapa perangkat lunak berbasis UNIX yang dapat digunakan untuk melakukan *IP filtering* antara lain *ipfwadm* (merupakan standar dari sistem Linux yang dapat diaktifkan pada level kernel) dan *ipchains* (versi baru dari *Linux kernel packet filtering* yang diharapkan dapat menggantikan fungsi *ipfwadm*).

Fungsi *proxy* dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya *web proxy, rlogin proxy, ftp proxy* dan sebagainya. Di sisi client sering kali dibutuhkan software tertentu agar dapat menggunakan *proxy server*, seperti dengan menggunakan *SOCKS*. Beberapa perangkat lunak berbasis UNIX untuk *proxy* antara lain *Socks* (proxy server oleh NEC Network Systems Labs) dan *Squid* (web proxy server).

Firewall bukan jaminan bahwa jaringan komputer yang menggunakan firewall akan aman seratus persen karena firewall sendiri dapat memiliki masalah seperti *Firewall Gauntlet* yang dibuat oleh Network Associates Inc. (NAI).[103] *Firewall Gauntlet* memiliki masalah sehingga dapat melewatkan koneksi dari luar yang seharusnya tidak boleh lewat padahal *Firewall Gauntlet* didengung-dengungkan oleh NAI sebagai *The World's Most Secure Firewall*.

e. Pemantau adanya serangan

Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tak diundang (*intruder*) atau adanya serangan (*attack*). Nama lain dari

[103] Lihat berita mengenai Firewall Gauntlet pada situs http://www.securityfocus.com/news/40

sistem ini adalah *intruder detection system* (IDS). Sistem ini dapat memberitahu administrator melalui e-mail maupun melalui mekanisme lain seperti pager. Ada beberapa cara untuk memantau adanya intruder, baik yang sifatnya akitf maupun pasif. IDS cara yang pasif misalnya dengan memonitor *log file*.

Ada beberapa contoh dari IDS, antara lain:

1) *Autobuse*, mendeteksi probing dengan memonitor log file
2) *Courtney* dan *portsentry*, mendeteksi *probing* (*port scanning*) dengan memonitor packet yang lalu lalang. *Portsentry* bahkan dapat memasukkan IP penyerang dalam *filter tcpwrapper*.
3) *Shadow* dari SANS
4) *Snort*, meneteksi pola (*pattern*) pada paket yang lewat dan mengirimkan *alert* jika pola tersebut terdeteksi. Pola-pola atau *rules* disimpan dalam berkas yang disebut *library* yang dapat dikonfigurasi sesuai dengan kebutuhan.

f. Pemantau integritas sistem

Sistem ini dijalankan secara berkala untuk menguji integritas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire*. Program ini dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya program ini dijalankan dan membuat database mengenai berkas-berkas atau direktori yang ingin kita amati beserta signature dari berkas tersebut. Signature berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil checksum atau hash dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hash function* akan berbeda dengan yang ada di database sehingga ketahuan adanya perubahan.

g. Audit: Mengamati berkas log

Segala kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasaynay disebut *log file* atau log saja. Berkas *log* ini sangat berguna untuk mengamati penyimpangan yang terjadi. Kegagalan untuk masuk ke sistem (*login*) misalnya tersimpan dalam berkas *log*. Untuk itu pada administrator diwajibkan untuk rajin memelihara dan menganalisa berkas *log* yang dimilikinya.

h. *Back up* secara rutin

Seringkali *intruder* masuk ke dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang ditemui. Jika *intruder* ini berhasil menjebol sistem dan masuk sebagai *super user*, maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu adanya *back up* yang dilakukan secara rutin merupakan sebuah hal yang essensial. Bayangkan jika yang berhasil dihapus oleh *intruder* itu adalah data-data rahasia apalagi data rahasia keamanan negara.

i. Penggunaan *Enkripsi* untuk meningkatkan keamanan

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi *enkripsi*. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di internet yang masih menggunakan plain text untuk *authenticaton* seperti penggunaan pasangan *userid* dan *password*. Informasi ini dapat dilihat dengan mudah oleh program penyadap atau pengendus (*sniffer*).

Untuk meningkatkan keamanan server *world wide web* dapat digunakan *enksipsi* pada tingkat *socket*. Dengan menggunakan enkripsi, orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang cukup populer adalah dengan menggunakan *Secure*

Socket Layer (SSL) yang mulanya dikembangkan oleh Netscape. Selain server WWW dari Netscape dapat juga dipakai server WWW dari Apache yang dapat dikonfigurasi agar memiliki fasilitas SSL dengan menambahkan software tambahan (SSLeay - implementasi SSL dari **Eric Young** - atau Open SSL - yaitu implementasi Open Source dari SSL). Penggunaan SSL memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku. Hal ini disebabkan karena pemerintah melarang ekspor teknologi enkripsi (*kriptografi*) dan paten *Public Key Partners* atas *Rivest-Shamir-Adleman* (RSA) *public key cryptography* yang digunakan pada SSL. Oleh karena itu implementasi SSLeay **Eric Young** tidakdapat digunakan di Amerika Utara (Amerika dan Kanada) karena melanggar paten RSA dan RC4 yang digunakan dalam implementasinya.

j. Telnet atau shell aman

Telnet atau *remote login* digunakan untuk mengakses sebuah remote site atau komputer melalui sebuah jaringan komputer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan userid dan password. Informasi tentang *userid* dan *password* ini dikirimkan melalui jaringan komputer secara terbuka. Akibatnya ada kemungkinan seorang yang nakal melakukan *sniffing* dan mengumpulkan informasi tentang pasangan *userid* dan *password* ini meskipun cara ini biasanya membutuhkan akses *root*.

Untuk menghindari hal ini, enkripsi dapat digunakan untuk melidungi adanya *sniffing*. Paket yang dikirimkan dienkripsi dengan algoritma DES atau *Blowish* (dengan menggunakan kunci session yang dipertukarkan via RSA atau *Diffie-Hellman*) sehingga tidak dapat dibaca oleh orang yang tidak berhal.. Salah satu implementasi mekanisme ini adalah SSH *(Secure Shell)*.

Dari beberapa responden yang berhasil ditemui, kebanyakan dari mereka tidak menggunakan sistem keamanan yang handal. Seperti dikatakan di atas, mereka menggunakan sistem keamanan yang murah dan sederhana, yaitu dengan menggunakan password. Password memang dapat (untuk sementara) mengamankan data-data yang ada dalam komputer, tetapi jangka atau kekuatan berlakunya password itu tidaklah lama karena alat-alat pemecah password dapat dengan mudah memecahkan password meskipun password tersebut sudah terenskripsi (*encrypted password*). Dengan kata lain pengamanan sistem informasi berbasis internet dengan menggunakan password sebenarnya merupakan atau berpotensi sebagai sumber lubang keamanan.

Password dapat saja menjadi sistem pengaman yang baik asalkan tidak membiarkan password itu digunakan untuk jangka waktu yang tidak terlalu lama dan selalu dalam pengawasan. Penggunaan password yang sama dan terlalu lama sangat berbahaya, karena dalam keadaan administrator lemah, *cracker* dapat masuk ke sistem dan mengeksploitasinya. Kelemahan dari pengelolaan password seperti ini terutama terjadi pada hari-hari di mana administrator libur atau pada hari-hari di mana jam kerja diliburkan.

Dari contoh kasus seperti itu maka penggunaan *One-Time Password* (OTP) merupakan pilihan bagi mereka. OTP didesain untuk mengatasi serangan dari pengguna jaringan yang tidak sah dan telah mendapatkan user ID beserta passwordnya melalui *packet sniffer* yang telah digunakan untuk melakukan *sniffing*. Desain OTP memaksa user jaringan untuk menggunakan password yang berbeda tiap kali melakukan *login*. Hal ini dapat dilakukan dengan cara menyediakan password untuk user jaringan yang berbeda tiap kali melakukan login. Akibat dari tindakan ini adalah sebuah password tidak dapat digunakan lebih dari satu kali.

Meskipun demikian, para korban umumnya masih khawatir menggunakan password dengan melihat pengalaman sebelumnya, sehingga mereka menginginkan sistem keamanan yang terbaik (paling tidak dapat tahan lama). Alternatif untuk ini adalah dengan menggunakan firewall, meskipun firewall terhitung mahal, mereka mulai mempertimbangkan untuk menggunakan alat pengaman ini untuk melindungi data-data penting. Resiko ini diambil karena mereka tidak ingin menjadi korban untuk yang kedua kali. Akan tetapi mereka juga harus ingat bahwa sampai sekarang belum ada jaminan sistem pengaman yang ada dapat menjamin situs yang dilindungi akan aman seratus persen, sehingga bagi mereka yang ingin berusaha melindungi situsnya harus secara terus menerus memperhatikan perkembangan sistem pengamanan internet ini.

Bagi korban *hacking* yang data-datanya telah dirusak atau dihapus oleh *cracker* dan masih mempunyai data *back up*, masalah kerusakan data dan sistem pengamanan bukanlah masalah yang terlalu sulit karena mereka dapat kembali mem*back up* data yang telah tersimpan di tempat lain ke situs yang telah diserang itu. Dengan kata lain, berapa kali pun *cracker* menyerang situs itu, maka dalam waktu yang tidak terlalu lama kerusakan itu akan teratasi dengan mem*back up* data-data yang tersedia dan situs dapat berjalan lagi seperti biasa. Tetapi jika hal ini berlangsung terus (mem*back up*) akan menjadi pekerjaan yang membosankan bagi administrator dan merupakan aib bagi webmaster, sehingga perencanaan sistem keamanan pada situsnya merupakan langkah yang perlu dipertimbangkan.

Menutup aplikasi atau servis-servis yang tidak digunakan juga merupakan langkah penting. Servis-servis seperti finger, telnet, ftp, smtp, pop, echo dan sebagainya, jika tidak perlu sekali sebaiknya ditutup karena servis-

servis itu merupakan sumber lubang keamanan. Meskipun servis-servis itu sudah ditutup, tetap saja ada *cracker* yang dapat masuk dan merusak sistem dan menghapus data yang ada (bahkan merusak servis-servis yang ditutup itu serta menghapus semua log file untuk menghilangkan jejak).

Meskipun sebuah sistem jaringan komputer telah diamankan dengan berbagai langkah-langkah seperti tersebut di atas, sekali lagi itu bukan jaminan jaringan komputer itu aman dari serangan *cracker*. Untuk memperkecil kemungkinan serangan itu dapat dilakukan dengan mengintegrasikan langkah-langkah pengamanan itu dan keakuratan serta keaktualan perkembangan sistem keamanan internet harus selalu terus diikuti. Tidak kalah penting dari semua itu adalah masalah pengawasan. Seorang administrator sistem harus secara kontinue mengawasi keluar masuknya para user atau tamu yang mengakses situs yang dikelolanya itu.

C. PERLINDUNGAN HUKUM TERHADAP PEMILIK WEBSITE DAN UPAYA KRIMINALISASI HACKING

1. Perlindungan Hukum Terhadap Pemilik Website

Perkembangan teknologi informasi yang berlangsung sangat cepat telah mempengaruhi hampir seluruh aspek kehidupan manusia, tidak terkecuali bidang hukum. Jaringan komunikasi global atau disebut juga Internet merupakan wahana bagi setiap orang untuk memanfaatkan dan menggunakan momentum ini sebagai jalan atau cara meningkatkan kesejahteraannya. Pemanfaatan dan penggunaan Internet sebagai media komunikasi untuk berbagai keperluan telah menjadi gejala yang mendunia (*mondial*).

Pemanfaatan dan penggunaan Internet secara meluas ini pada satu sisi membawa perubahan paradigma pada bidang kehidupan yang positif, seperti bidang bisnis, politik, sosial, budaya dan sebagainya, tetapi pada sisi lain juga menimbulkan perubahan paradigma dalam studi mengenai kejahatan. Kajian kriminologi yang ada saat ini merupakan kajian terhadap kejahatan yang terjadi di dunia nyata (*physical world* atau *real life*), sedangkan penggunaan dan pemanfaatan Internet menimbulkan dimensi baru kejahatan yang terjadi di dunia maya (*virtual reality*). Kajian kriminologis mengenai kehidupan dunia maya ini sangat perlu dilakukan mengingat harapan-harapan yang digantungkan begitu tinggi pada Internet. Kajian kriminologis terhadap kehidupan maya makin semakin mengukuhkan sebuah pendapat bahwa di dunia maya, yang realitasnya adalah realitas virtual, dan komunitasnya berupa komunitas virtual ternyata memiliki penjahatnya sendiri.

Negara-negara yang menjadi pioneer dalam bidang ini telah merespon perkembangan abad informasi ini dengan mengubah berbagai paradigma yang meliputi pemanfaatan dan penggunaan Internet dalam perundang-undangan yang terkait. Meski demikian, perkembangan Internet begitu pesat sehingga perubahan itu harus secara terus menerus diperhatikan agar perundang-undangan yang terbentuk betul-betul dapat mengakomodasi dan melindungi berbagai kepentingan yang terkait.

Negara-negara berkembang dan terbelakang (termasuk Indonesia) yang umumnya tertinggal dalam pengembangan dan pemanfaatan teknologi informasi, merasa kesulitan untuk merumuskan suatu perundang-undangan yang mengatur aktivitas di *cyberspace*. Di saat kesulitan dalam menyusun

perundang-undangan itu, serbuan Internet dan pemanfaatannya di berbagai bidang tidak bisa dibendung, sehingga dalam menghadapi hal ini dimunculkan pemikiran untuk menggunakan hukum positif yang ada (*the existing law*).

Memang diakui sendiri oleh Menteri Kehakiman waktu itu **Yusril Ihza Mahendra**, Indonesia sampai saat ini belum memiliki pengaturan khusus mengenai *cyberspace* atau *cyber world*. Keadaan ini diakuinya bukan berarti pemerintah kurang peka terhadap perkembangan teknologi informasi (lebih tepatnya tertinggal), tetapi lebih disebabkan karena pengaturan mengenai *cyberspace* memerlukan kajian-kaijan yang cermat dan mendalam, agar benar-benar tepat sasaran sesuai dengan tingkat perkembangan perilaku kehidupan masyarakat, sehingga tidak akan menimbulkan stagnasi di dalam implementasinya.[104]

Penggunaan hukum positif yang ada untuk kejahatan atau perbuatan yang secara paradigmatis memiliki perbedaan tentunya tidak membawa keberuntungan bagi berbagai pihak. Perundang-undangan lama (hukum positif saat ini) memiliki paradigmanya sendiri yang melandasi pembuatan atau penciptaan perundang-undangan itu yang disesuaikan dengan jamannya, sedangkan sekarang jaman telah berubah. Konsep ruang dan waktu yang telah melandasi pembuatan hukum positif telah didobrak dengan perkembangan Internet. Pendobrakan terhadap konsep ruang dan waktu ini seharusnya diikuti dengan pendobrakan terhadap sistem hukum yang masih mendasari pada konsep itu.

---

104 Yusril Ihza Mahendra, *Regulasi Cyberspace Di Indonesia*, Makalah pada Seminar tentang *Cyber* Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000, hal. 3

Meskipun demikian membuat perundang-undangan (apalagi mengubah paradigma pemikiran dari para pembuatnya) tidaklah semudah membalik telapak tangan. Untuk hal ini butuh proses dan proses itu tidak dapat dipastikan kapan berakhirnya, sehingga harapan untuk memiliki perundang-undangan yang mengatur kegiatan di *cyberspace* hanya akan tinggal harapan jika proses yang dimaksud tidak kunjung selesai.

Memberikan perlindungan kepada warganegara dengan harta bendanya merupakan kewajiban pemerintah. Meskipun undang-undang yang mengatur kegiatan di *cyberspace* belum ada, sedangkan sebagian warganegara yang ada telah menggunakan Internet untuk berbagai keperluan, maka secara moril pemerintah memiliki kewajiban untuk melindungi warganegaranya tersebut. Perlindungan ini tentunya diberikan dengan memanfaatkan atau memberlakukan perundang-undangan yang ada dengan berbagai cara seperti penafsiran maupun analogi. Tetapi apakah tepat hal ini diterapkan, inilah pertanyaan yang harus ditemukan jawabannya.

Badan Pembinaan Hukum Nasional dalam sebuah penerbitannya mencoba untuk mengidentifikasikan bentuk-bentuk kejahatan yang berkaitan dengan aktivitas di *cyberspace* dengan perundang-undangan pidana yang ada. Hasil identifikasi itu berupa pengkategorian perbuatan kejahatan *cyber* (*cybercrime*) ke dalam delik-delik dalam KUHP sebagai berikut:[105]

a. *Joycomputing*, diartikan sebagai perbuatan seseorang yang menggunakan komputer secara tidak sah atau tanpa ijin dan menggunakannya melampaui wewenang yang diberikan. Tindakan ini dapat dikategorikan sebagai tindak pidana pencurian (Pasal 362 KUHP);

---

[105] Badan Pembinaan Hukum Nasional, *Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi*, BPHN Departemen Kehakiman R.I., 1995/1996, hal. 32-34

b. *Hacking*, diartikan sebagai suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa ijin (dengan melawan hukum) dari pemilik sah jaringan komputer tersebut. Tindakan ini dapat dikategorikan sebagai tindak pidana perbuatan tanpa wewenang masuk dengan memaksa ke dalam rumah atau ruangan yang tertutup atau pekarangan atau tanpa haknya berjalan di atas tanah milik orang lain (Pasal 167 dan 551 KUHP);

c. *The Trojan Horse*, diartikan sebagai suatu prosedur untuk menambah, mengurangi atau mengubah instruksi pada sebuah program, sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melaksanakan tugas lain yang tidak sah. Tindakan ini dapat dikategorikan sebagai tindak pidana penggelapan (Pasal 372 dan 374 KUHP). Apabila kerugian yang ditimbulkan menyangkut keuangan negara, tindakan ini dapat dikategorikan sebagai tindak pidana korupsi.

d. *Data Leakage*, diartikan sebagai pembocoran data rahasia yang dilakukan dengan cara menulis data-data rahasia tersebut ke dalam kode-kode tertentu sehingga data dapat dibawa ke luar tanpa diketahui oleh pihak yang bertanggung jawab. Tindakan ini dapat dikategorikan sebagai tindak pidana terhadap keamanan negara (Pasal 112, 113 dan 114 KUHP) dan tindak pidana membuka rahasia perusahaan atau kewajiban menyimpan rahasia profesi atau jabatan (Pasal 322 dan 323 KUHP).

e. *Data diddling*, diartikan sebagai suatu perbuatan yang mengubah data valid atau sah dengan cara yang tidak sah, yaitu dengan mengubah *input data* atau *output data*. Tindakan ini dapat dikategorikan sebagai tindak pidana pemalsuan surat (Pasal 263 KUHP)

f. Penyia-nyiaan data komputer, diartikan sebagai suatu pebuatan yang dilakukan dengan suatu kesengajaan untuk merusak atau menghancurkan media disket dan media penyimpanan sejenis lainnya yang berisikan data atau program komputer, sehingga akibat perbuatan tersebut data atau program yang dimaksud menjadi tidak berfungsi lagi dan pekerjaan-pekerjaan yang melalui program komputer tidak dapat dilaksanakan. Tindakan ini dapat dikategorikan sebagai tindak pidana perusakan barang (Pasal 406 KUHP).

Apa yang dilakukan oleh BPHN sudah cukup baik meskipun baru sebatas pemikiran untuk menanggulangi kekosongan hukum. Tetapi sebagaimana disebutkan di atas, perbedaan konsep mengenai ruang dan waktu dari perundang-undangan pidana dengan sifat Internet akan membawa kesulitan dalam penerapannya, bahkan untuk beberapa pasal, penerapan KUHP terhadap beberapa aktivitas di *cyberspace* patut untuk dipertanyakan.

Pertanyaan-pertanyaan ini muncul berkaitan dengan berlakunya asas perlindungan (asas nasional pastif) dan asas universal dalam KUHP. Misalnya mengenai penerapan Pasal 282 KUHP yang mengatur penyiaran tulisan atau gambar yang melanggar kesopanan (pornografi). Sebelum adanya Internet, pasal ini sudah menjadi perdebatan, dan kini dengan adanya internet yang menawarkan situs porno, pasal ini kembali diperdebatkan terutama mengenai batasan di muka umum. Apakah layar komputer yang menampilkan gambar dari situs porno dapat dikatakan sebagai unsur di muka umum. Selain itu adalah Pasal 154 KUHP mengenai *haatzaai artikelen*, apakah penyebaran kebencian terhadap Pemerintah Republik Indonesia yang sah di Internet dapat dikategorikan sebagai *haatzaai artikelen*. Bagaimana jika para pelaku (baik

penyebar gambar porno ataupun penyebar kebencian terhadap Pemerintah Republik Indonesia) berada di luar negeri, sedangkan jika pelaku di Indonesia saja sulit untuk dilacak karena para pelaku umumnya tidak mencantumkan alamat yang jelas selain alamat di dunia maya.[106]

Meskipun telah diusahakan untuk menggunakan hukum pidana positif yang ada, hanya beberapa kasus yang dapat ditangani dan diputus oleh pengadilan,[107] sedangkan berdasarkan data-data yang diungkapkan pada bagian sebelumnya, korban-korban (terutama hacking) telah berjatuhan. Reaksi masyarakatpun bermunculan sehingga hal ini menimbulkan pertanyaan dalam benak setiap orang yang berminat terhadap penegakan hukum di *cyberspace*. Bagaimana kerja aparat kepolisian sebenarnya.

Polri oleh **Didi Widayadi** sering dilukiskan selalu dinamis dan berkembang sesuai dengan situasi dan kondisi masyarakat.[108] Tetapi dalam menghadapi kejahatan *cybercrime* ini, Polri terkesan kurang dinamis. Kasus-kasus yang berkaitan dengan *cybercrime* dan ditangani oleh Polri bukan murni hasil kerjaan Polri karena hanya didasarkan pada laporan dari korban.

---

106 Penjelasan dan berbagai pertanyaan mengenai hal-hal seperti itu khususnya yang berkaitan dengan kebebasan pers di Indonesia dalam kaitannya dengan *cyber* communication dapat dibada dalam makalah Khrisna Harahap. *Kebebasan Pers Di Indonesia Memasuki Cyber Communication*, Makalah pada Seminar Nasional mengenai *Cyberlaw*, diselenggarakan oleh Sekolah Tinggi Hukum Bandung (STHB) di Bandung, 9 April 2001.

107 Kasus yang dimaksud adalah kasus kejahatan komputer perbankan BNI 1946 yang dilakukan oleh Rudy Demsy dengan Putusan PN Jakarta Pusat No. 135/X/Pid/B/1987; Putusan PT. DKI Jakarta No. 94/Pid/1988 dan Putusan MARI No. 1852.K./Pid/1988; kasus Bank Rakyat Indonesia (BRI) Cabang Brigjen Katamso, Yogyakarta dan Kasus Bank dagang Negara Cabang Jakarta Bintaro Jaya.

108 Didi Widayadi, Irjen Pol adalah Kadisinfolahta Polri. Didi Widayadi, *Kebijakan dan Strategi Operasional POLRI Dalam Kaitan Hakekat Ancaman Cybercrime*, Makalah pada Seminar tentang *Cyber* Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000, hal. 2

Beberapa kasus penting yang pernah ditangani Polri di bidang *cybercrime* di antaranya adalah:[109]

a. *Cyber Smuggling*, berupa laporan pengaduan dari US Custom (Pabean AS) adanya tindak penyelundupan via internet yang dilakukan oleh beberapa orang Indonesia, di mana oknum-oknum tersebut telah mendapatkan keuntungan dengan melakukan *Webhosting* gambar-gambar porno di beberapa perusahaan *Webhosting* yang ada di Amerika Serikat;
b. Pemalsuan Kartu Kredit berupa laporan pengaduan dari warganegara Jepang, Prancis dan Amerika[110] tentang tindak pemalsuan kartu kredit yang mereka miliki untuk keperluan transaksi di Internet
c. *Hacking* situs, hacking beberapa situs termasuk situs POLRI yang pelakunya diidentifikasikan berada di Indonesia.

Seperti disebutkan di atas, kasus-kasus tersebut bukan murni hasil penyidikan Polri. Hal ini dapat menjadi pertanyaan sampai sejauh mana kemampuan Polri dalam menganggulangi *cybercrime* apalagi jika dikaitkan dengan kasus yang menimpa Polri sendiri yaitu ketika situs Polri dihack pada Juni 1999 dan 8 Mei 2001, yang penanganannya sampai sekarang tidak kunjung usai.

Ketidakmampuan Polri dalam mengungkap *cybercrime* ini diakui sendiri oleh **Didi Widayadi** mengingat keterbatasan yang dimiliki oleh Polri pada saat ini. Kesan atau stigma ketidakmampuan Polri inilah yang menyebabkan para korban hacking enggan melaporkan kasusnya kepada Polri. Keterbatasan ini

---

109 *Ibid.*

110 Lihat beritanya di Suara Merdeka dengan judul *Reserse Polda Jateng Ungkap Kejahatan Internasional Internet*, 17 November 2000.

oleh Polri hendak dihilangkan dengan menerapkan beberapa langkah, antara lain:[111]

a. Landasan Hukum

Landasan hukum yang menjadi acuan bagi Polri dalam menghadapi hakekat ancaman *cybercrime* sementara ini masih menggunakan KUHP, padahal permasalahan yang dihadapi oleh Polri adalah ancaman hukum untuk pelaku *cybercrime* dengan menggunakan KUHP tidak efektif. Ancaman hukuman di KUHP dibandingkan dampak dari hasil *cybercrime* tidak berimbang.

b. Organisasi

Satuan Kerja dalam Polri yang mempunyai kewenangan penuh dalam melakukan penyelidikan dan penyidikan tindak pidana adalah Reserse, hanya saja satuan kerja dalam Reserse tersusun untuk menangangi kejahatan yang bersifat fisik, sementara *cybercrime* merupakan kejahatan yang bersifat non fisik (maya). Akibatnya dalam melaksanakan tugasnya Reserse Polri mengalami hambatan. Namun demikian sejak 1999 di Dinas Informasi dan Pengolahan Data Polri telah dibentuk satu sub dinas yang bernama Sub Dinas Bantuan Operasional (Banops) yang salah satu tugasnya memberikan dukungan teknis untuk penanganan *cybercrime*.[112]

---

111 Ibid, hal. 3-5

112 Langkah Polri ini sebenarnya cukup bagus, tetapi hasil yang nampak tidak menggembirakan karena sifat kerjanya tidak total dan hanya bersifat bantuan, sehingga dalam hal ini Polri bisa mencontoh India yang telah membentuk Polisi Saiber yang dinamakan *The National Cyber Cop Committee* atau *Computer Emergency Response Team* (CERT) yang dibentuk oleh DARPA pada tahun 1988 atau dapat juga meniru apa yang dilakukan oleh FBI dengan membentuk FBI *Cybercrime Investigation Capabilities* yang meliputi *National Infrastructure Protection Center, National Infrastructure Protection and Computer Intrusion Squads/Teams*, dan sebagainya. Mengenai badan atau lembaga yang ada di FBI yang berkaitan dengan cybercrime dapat dilihat lebih jelas pada Louis J. Freeh, Statemen of the Record on *Cybercrime*, Februaty 16, 2000, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress03.htm

c. Sumberdaya Manusia

Dalam menghadapi ancaman *cybercrime* oleh Polri disadari bahwa sumberdayanya harus dibenahi mengingat di masa mendapat prediksi jumlah kejahatan ini akan meningkat baik secara kuantitas maupun kualitas. Langkah-langkah yang diambil Polri untuk meningkatkan kesiapan sumberdaya manusia antara lain:

1) Mengkursuskan anggota untuk meningkatkan kemampuan di bidang teknologi informasi;
2) Mengupayakan mendapatkan bantuan pendidikan di bidang penanganan *cybercrime* dari negara-negara maju, seperti Amerika, Jepang, Prancis, Inggris. Upaya ini sudah mendapat kemajuan antara lain dari US Custom (Pabean Amerika) yang siap melatih tenaga-tenaga dari Polri untuk penanganan *cybercrime*.
3) Melakukan *recruitment Outsourcing* dari kalangan individu, swasta, perguruan tinggi yang mempunyai komitmen ingin membantu Polri. Beberapa tenaga Lembaga Penelitian Universitas Indonesia semenjak tahun 1998 telah ikut membantu Polri.

Langkah-langkah yang dilakukan oleh Polri ini sangat baik untuk masa mendatang, sedangkan untuk masa kini tampaknya kesan terhadap Polri seperti tersebut di atas tampaknya masih akan terus melekat. Hal ini didasarkan kepada alasan bahwa hukum mengenai *cybercrime* sampai saat ini belum ada dan tidak dapat diprediksi kapan ada, sedangkan Polri bekerja berdasarkan landasan hukum. Ketiadaan landasan hukum ini menyebabkan Polri tidak dapat bergerak lebih jauh karena dengan menerapkan hukum pidana positif yang ada (KUHP)

dianggapnya tidak efektif. Keadaan ini tentu saja semakin membuka peluang bagi para cracker untuk melakukan aksinya.

Keadaan ini sebenarnya bisa dihindari jika Polri berani mengambil sikap mempergunakan hukum yang tidak tertulis yang hidup di *cyberspace*, misalnya menggunakan etika hacker ataupun menggunakan hukum pidana positif meskipun ancaman pidananya tidak sebanding dengan akibat yang ditimbulkan *cybercrime*. Langkah ini paling tidak menunjukkan bahwa Polri mau dan mampu serta mempunyai komitmen dalam menghadapi *cybercrime*.

Ketidakmampuan Polri dalam mengungkap *cybercrime* dan menangkap pelakunya menyebabkan korban enggan untuk melaporkan kasusnya ke Polri. Langkah yang paling tepat bagi korban adalah melakukan langkah *preventif* (pencegahan) dengan memasang sistem keamanan yang baik dan langkah *recovery* (pengobatan) dilakukan sendiri dengan memback up data yang hilang atau membangun kembali situs yang dihack itu. Keterlibatan Polri dalam langkah *recovery* ini oleh korban tidak diharapkan karena dianggap tidak akan membawa pengaruh apa-apa kecuali pengaruh buruk bagi korban (perusahaan dan *webmaster*nya) karena terpublikasikannya situs yang dimiliki dan dikelolanya itu.

Dari hal ini dapat disimpulkan bahwa sampai saat ini pemerintah tidak memberikan perlindungan hukum apapun terhadap pemilik atau pengelola situs baik yang telah menjadi korban ataupun yang tidak. Kesimpulan ini didasarkan pada dua pendapat. *Pertama* pendapat para korban yang telah mengalami sendiri aktivitas cracker dan sama sekali tidak ada tindakan apapun dari pemerintah (aparat penegak hukum) meskipun situs yang telah menjadi korban

itu milik pemerintah. *Kedua* adalah kinerja Polri yang selalu didasarkan pada hukum tertulis serta keengganannya menggunakan hukum pidana positif yang ada sehingga ketika hukum tertulis yang dimaksud belum atau tidak ada maka Polri tidak atau kurang memperhatikan masalah *cybercrime*, di samping itu sumberdaya yang ada dalam tubuh Polri juga menjadi salah satu alasannya.

2. Upaya Kriminalisasi Terhadap Hacking

Secara radikal, *cyberspace* telah mengubah hubungan antara *legally significant (online) phenomena and physical location*. Peningkatan jaringan komputer global (*global computer network*) telah menghancurkan hubungan antara letak geografis dengan:

a. kewenangan pemerintah untuk memaksakan kontrol atas *online behaviour;*

b. pengaruh *online behaviour* terhadap individu atau barang;

c. legitimasi pemerintah untuk mengatur fenomena global; dan

d. kemampuan wilayah untuk memberitahukan kepada orang yang melewati perbatasan mengenai hukum yang berlaku.[113]

Perubahan yang radikal ini sebagaimana dikatakan oleh **Jessica Lipnack** dan **Jeffrey Stamps** merupakan *smash the boundaries, tear down the hierarchy and dismantle the bureaucracy*. Tentunya perubahan ini menyebabkan apapun yang bersentuhan dengan teknologi informasi ini mengalami penyesuaian. Tidak hanya itu, ketika teknologi informasi dikatakan sebagai kekuatan yang besar, ia bergerak dengan kebesarannya melakukan penyebaran ke seluruh dunia tanpa sekalipun ada yang mengatakan bahwa hal ini merupakan

---

[113] David R. Johnson dan David Post sebagaimana dikutip dalam Naskah Akademik Rancangan Undang-undang Tentang Teknologi Informasi, Prakarsa Direktorat Jenderal Pos dan Telekomunikasi, Departemen Perhubungan RI dengan FH UNPAD Bandung, 2000, hal 38

kolonialisme baru. Teknologi informasi berhasil menancapkan kaki-kakinya tanpa disadari oleh masyarakat dan mengubah perilakunya.

Di negara-negara berkembang dan terbelakang, pengguna atau pemakai internet umumnya terpusat di kota-kota besar karena struktur dan infrastruktur telekomunikasi lebih mudah didapat sedangkan di daerah pedesaan teknologi informasi masih merupakan barang baru. Meski demikian perkembangan pengguna internet menunjukkan angka yang signifikan.

Teknologi informasi tidak akan menjadi besar tanpa bantuan dari pihak lain sebagai pengembang, pemasar dan pengguna. Paling tidak ada tiga pihak yang kemudian saling menyesuaikan diri menuju apa yang sekarang populer dengan istilah dunia maya atau *virtual reality* atau mayantara atau disebut juga *electronic world.* *Pertama* adalah kemauan dan masyarakat untuk menggunakannya teknologi informasi ini. Dalam hal ini masyarakat merupakan pengguna dan dalam optik ekonomi merupakan pangsa pasar. *Kedua*, dalam rangka menyongsong pemanfaatan teknologi informasi untuk berbagai bidang, maka industri teknologi informasi harus mempersiapkan diri, artinya industri yang bergerak di bidang teknologi informasi harus mempersiapkan diri apabila terjadi permintaan sarana dan prasarana internet. *Ketiga*, kesiapan pemerintah masing-masing negara (terutama negara-negara berkembang dan terbelakang) untuk menerima era internet sebagai bagian penting dari kehidupan.

Kesiapan pemerintah dalam hal ini tidak hanya menyangkut persiapan dalam pemanfaatan teknologi informasi untuk pelayanan publik sebagaimana tugas-tugas pemerintahan, tetapi juga persiapan dalam menyediakan perangkat hukum yang mengatur aktivitas di *cyberspace*, termasuk kesiapan dalam

menanggulangi kejahatan yang timbul sebagai akibat penggunaan dan pemanfaatan teknologi informasi untuk kepentingan yang tidak bertanggung jawab atau melanggar hukum.

Kejahatan selalu ada di muka bumi ini dan diciptakannya Internet yang semula diperuntukkan bagi kegiatan-kegiatan yang bersifat positif (penelitian, pendidikan, bisnis, dan sebagainya) ternyata telah dimanfaatkan pula untuk melakukan kejahatan. Teknologi di samping memberikan kemudahan-kemudahan ternyata mempunyai sifat kriminogen. Hal ini tidak terungkap dalam Kongres PBB keempat tahun 1970 yang diselenggarakan di Kyoto, Jepang tentang pencegahan kejahatan dan pembinaan para pelaku (*Forth United Nations Congress on the Prevention of Crime and the Treatment of Offender*). Kongres tidak dapat menetapkan dengan pasti hubungan antara kejahatan dan perkembangan (*development*), sehingga menurut kongres tidak beralasan untuk mengatakan bahwa perkembangan masyarakat mencegah terjadinya kejahatan atau sebaliknya bahwa perkembangan itu menyebabkan kejahatan. Akan tetapi kongres mengakui bahwa beberapa aspek penting dari perkembangan masyarakat dianggap potensial sebagai kriminogen, artinya mempunyai kemungkinan untuk menimbulkan kejahatan. Aspek-aspek ini adalah urbanisasi, industrialisasi, pertambangan penduduk, perpindahan penduduk setempat, mobilitas sosial dan ***perubahan teknologi***. Hal-hal ini diangap demikian karena mempunyai pengaruh secara tidak langsung terhadap perilaku sikap tindak dari beberapa golongan masyarakat.[114]

---

[114] Kongres PBB Keempat sebagaimana dikutip oleh Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1986, hal. 94. Hal senada juga diungkapkan oleh Muladi yaitu kemajuan teknologi masyarakat (*technological advance of society*) seringkali membawa dampak sampingan antara lain kejahatan komputer. Muladi dalam Muladi dan Barda Nawawi Arief, *Bunga Rampai Hukum Pidana*, Alumni, Bandung, 1992, hal. 4

Selain Kongres tersebut, PBB juga melakukan Kongres berikutnya dalam rangka membahas mengenai kejahatan yang menggunakan komputer sebagai sarananya. Kongres PBB mengenai *The Prevention of Crime and the Treatment of Offender* ke 8 tahun 1990 di Havana, Kuba dan Kongres ke 10 di Wina. Pada Kongres ke 8 PBB memandang perlu dilakukan usaha-usaha penanggulangan kejahatan yang berkaitan dengan komputer (*computer related crime*). Usaha-usaha ini kemudian dilanjutkan pada Kongres ke 10 di Wina.

Berbicara mengenai kejahatan (*crime*), tidak dapat dilepaskan dari lima faktor yang saling tali temali, yaitu pelaku kejahatan, modus kejahatan, korban kejahatan, reaksi sosial atas kejahatan dan hukum. Hukum memang menjadi instrumen penting dalam pencegahan dan penanggulangan kejahatan, di samping instrumen-instrumen lain yang juga tidak kalah penting. Akan tetapi untuk membuat suatu ketentuan hukum terhadap bidang yang berubah sangat cepat seperti teknologi informasi ini bukanlah suatu perkara yang mudah. Di sinilah seringkali hukum (peraturan) tampak cepat menjadi usang manakala mengatur bidang yang mengalami perubahan cepat, sehingga situasinya seperti terjadi kekosongan hukum (*vaccum rechts*). Terhadap kejahatan di internet atau *cybercrime* ini nampaknya memang terjadi kekosongan hukum. [115]

Perkembangan yang pesat dalam teknologi Internet itu menyebabkan kejahatan baru di bidang itu juga muncul, misalnya kejahatan manipulasi data, spionasi, sabotase, provokasi, *money laundering, hacking*, pencurian *software* maupun perusakan hardware dan berbagai macam lainnya. Bahkan laju kejahatan melalui jaringan internet (*cybercrime*) tidak diikuti dengan kemampuan pemerintah untuk mengimbanginya sehingga sulit untuk

---

[115] Tb. Ronny R. Nitibaskara, *Problema Yuridis Cybercrime*, Makalah pada Seminar tentang *Cyber* Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000, hal. 2 dan 5

mengendalikannya. Munculnya beberapa kasus *cybercrime* di Indonesia telah menjadi ancaman stabilitas kamtibmas dengan eskalatif yang cukup tinggi. Pemerintah dengan perangkat hukum hampir tidak mampu mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer khususnya di jaringan internet dan intranet (*internetwork*).[116]

Internet di samping menjanjikan sejumlah harapan dan keuntungan, juga melahirkan kecemasan-kecemasan baru dengan munculnya kejahatan yang lebih canggih dalam bentuk *cybercrime*.[117] Sebagai contoh adalah aktivitas hacking yang menimbulkan resiko yang tinggi, apalagi jika yang dihack itu menyangkut jaringan informasi institusi atau instalasi vital seperti halnya pusat-pusat penelitian, jaringan sistem informasi bisnis keuangan dan perbankan, reaktor nuklir, sistem pertahanan keamanan negara, pengawas penerbangan pesawat udara atau jaringan-jaringan komputer rumah sakit dan medis.

Mengingat sifat Internet yang melampaui batas negara, memecahkan masalah waktu dan tempat dan beroperasi di dunia maya, Internet melahirkan berbagai bentuk kegiatan yang tidak sepenuhnya di atur oleh hukum yang berlaku saat ini (*the existing law*). Kenyataan ini telah menyadarkan

---

116 Didi Widayadi, *op.cit.*, hal. 1-2

117 Kecemasan atau kekhawatiran ini terungkap dari sebuah makalah yang disampaikan pada Information Technology Association of Canada (ITAC) yang berjudul "IIIC Commmon Views Paper On: Cyber Crime", IIIC 2000 Millenium Congress, September 19th, 2000, hal. 20 yang menyatakan Cybercrime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can electronically enabled crime. Lihat dalam Barda Nawawi Arief, Kebijakan Kriminalisasi dan Masalah Jurisdiksi Tindak Pidana Mayantara, Makalah pada Seminar Nasional Teknologi Informasi (Cyberlaw), Kerjasama Ditjen Postel dan UNDIP Semarang, 26 Juli 2001, hal. 2. European Council juga memandang masalah cybercrime merupakan bagian sisi paling buruk dari masyarakat informasi (Cyber crime is part of the scamy side of the Information Society). Keterangan lebih jelas mengenai sikap Europe Council ini dapat dilihat di http://convention.coe.int/a29opinion301.pdf mengenai Article 29 Working Group Opinion 4/2001, On the Council of Europe's Draft Convention on Cyber-crime, 22 March 2001.

masyarakat akan perlunya regulasi yang mengatur mengenai aktivitas di internet.[118]

Urgensi pengaturan nasional atas kegiatan-kegiatan di *cyberspace* dilandasi oleh 3 (tiga) pemikiran utama, yaitu:[119]

a. perlunya kepastian hukum bagi para pelaku kegiatan-kegiatan di *cyberspace* dikarenakan belum diakomodasikan secara memadai dalam regulasi yang telah ada;
b. upaya untuk mengantisipasi implikasi-implikasi yang ditimbulkan akibat pemanfaatan teknologi informasi; dan
c. adanya variabel global yaitu persaingan bebas dan pasar terbuka (WTO/GATT)

Aktivitas di Internet tidak bisa dilepaskan dari manusia dan akibat hukumnya terhadap manusia yang ada di dalam kehidupan nyata (*real life physical world*) sehingga muncul pemikiran mengenai perlunya aturan hukum untuk mengatur aktivitas tersebut. Internet memiliki karakteristik yang berbeda dengan dunia nyata sehinga muncul pro dan kontra mengenai bisa tidaknya hukum tradisional/konvensional (*the existing law*) mengatur aktivitas tersebut atau perlu tidaknya aktivitas di internet di atur oleh hukum. Permasalahan sebenarnya bukan sebatas pada eksistensi hukum tradisional dalam mengatur aktivitas di Internet, melainkan mempertanyakan eksistensi sistem hukum tradisional dalam mengatur aktivitas di Internet.[120]

---

118 Atip Latifulhayat, *Cyberlaw dan Urgensinya Bagi Indonesia*, Makalah pada Seminar tentang *Cyber* Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000, hal. 3.

119 Mieke Komar Kantaatmaja, *Meyongsong Penyusunan Peraturan Perundang-undangan Telematika (Cyberlaw)*, Makalah pada Seminar Nasional tentang Aspek Hukum Transaksi Perdagangan via Internet di Indonesia (E-Commerce) diselenggarakan oleh SEMA FH Unpad, Bandung, 22 Juli 2000, hal. 7.

120 Atip Latifulhayat, *op.cit*, hal. 4

Pro kontra tersebut disebabkan oleh 2 (dua) hal, pertama, karakteristik aktivitas di Internet yang bersifat lintas batas, sehingga tidak lagi tunduk pada batasan-batasan teritorial, kedua, sistem hukum tradisional yang justru bertumpu pada batasan-batasan teritorial dianggap tidak cukup memadai untuk menjawab persoalan-persoalan hukum yang muncuk akibat aktivitas di Internet. Pro kontra mengenai masalah ini sedikitnya terbagi menjadi tiga kelompok, yaitu:[121]

a. Kelompok pertama secara total menolak setiap usaha untuk membuat aturan hukum bagi aktivitas-aktivitas di Internet yang didasarkan atas sistem hukum tradisional. Mereka beralasan bahwa Internet yang layaknya sebuah surga demokrasi (*democratic paradise*) yang menyajikan wahana bagi adanya lalu lintas ide secara bebas dan terbuka tidak boleh dihambat dengan aturan yang didasarkan atas sistem hukum tradisional yang bertumpu pada batasan-batasan teritorial. Dengan pendirian seperti ini, maka menurut kelompok ini Internet harus diatur sepenuhnya oleh sistem hukum baru yang didasarkan atas norma-norma hukum yang baru pula yang diangap sesuai dengan karakteristik yang melekat pada Internet. Kelemahan utama dari kelompok ini adalah mereka menafikan fakta, meskipun aktivitas Internet itu sepenuhnya beroperasisecara virtual, tetapi masih tetap melibatkan masyarakat (manusia) yang hidup di dunia nyata.
b. Kelompok kedua berpendapat bahwa penerapan sistem hukum tradisional untuk mengatur aktivitas-aktivitas di Internet sangat mendesak untuk dilakukan. Tanpa harus menunggu akhir dari suatu perdebatan akademis mengenai sistem hukum yang paling tepat untuk mengatur aktivitas di

---

121 *Ibid*, hal. 4-6

Internet. Pertimbangan pragmatis yang didasarkan atas meluasnya akibat yang ditimbulkan oleh Internet memaksa untuk segera membentuk aturan hukum mengenai hal tersebut. Untuk itu semua yang paling mungkin adalah dengan mengaplikasikan sistem hukum tradisinal yang saat ini berlaku. Kelemahan utama kelompok ini merupakan kebalikan dari kelompok pertama yaitu mereka menafikan fakta bahwa aktivitas-aktivitas di Internet menyajikan realitas dan persoalan baru yang merupakan fenomena khas masyarakat informasi yang tidak sepenuhnya dapat direspon oleh sistem hukum tradisional.

c. Kelompok ketiga tampaknya merupakan sintesis dari kedua kelompok di atas. Mereka berpendapat bahwa aturan hukum yang akan mengatur mengenai aktivitas di Internet harus dibentuk secara evolutif dengan cara menerapkan prinsip-prinsip *common law* yang dilakukan secara hati-hati dan dengan menitikberatkan kepada aspek-aspek tertentu dalam aktivitas *cyberspace* yang menyebabkan kekhasan dalam transaksi-transaksi di Internet. Kelompok ini memiliki pendirian yang cukup moderat dan realistis, karena memang ada beberapa prinsip hukum tradisional yang masih dapat merespon persoalan hukum yang timbul dari aktivitas Internet di samping juga fakta bahwa beberapa transaksi di Internet tidak dapat sepenuhnya direspon oleh sistem hukum tradisional. **Atip Latifulhayat** termasuk yang setuju dengan pendirian kelompok ini, sehingga pemahamannya mengenai *cyberlaw* didasarkan atas satu konstruksi hukum yang mensintesiskan prinsip-prinsip hukum tradisional dengan norma-norma hukum baru yang terbentuk akbiat dari aktivitas-aktivitas manusia lewat Internet.

Sebenarnya masih ada kelompok keempat yang menolak sama sekali regulasi di *cyberspace*. Penolakan ini didasarkan pada asumsi bahwa *cyberspace* adalah ruang yang bebas, dan pemerintahpun tidak berhak untuk melarang sesuatu tindakan apapun di *cyberspace* itu. Landasan utama dari kelompok ini adalah *Declaration of Independence of Cyberspace* dari **John Perry Barlow** dan *Hacker Manifesto* dari **Loyd Blankeship** atau **The Mentor.**

Sehubungan bentuk pengaturan di dalam *cyberspace*, dapat ditinjau dari dua pendekatan, yaitu pertama apakah perlu menciptakan norma-norma dan peraturan-peraturan khusus untuk kegiatan/aktivitas di *cyberspace* atau *cyberlaw* dan kedua perlu diterapkan model-model peraturan yang dikenal di dunia nyata pada dunia *cyber*.[122] Untuk menentukan model mana yang sebaiknya dipakai maka perlu ditentukan terlebih dahulu ruang lingkup dari *cyberlaw*.

Sebelum membahas mengenai ruang lingkup *cyberlaw*, perlu diperhatikan bahwa istilah *cyberlaw* sebagai hukum yang mengatur aktivitas di *cyberspace* bukanlah istilah yang baku. Isitlah-istilah yang sepadan atau sinonim dengan *cyberlaw* di antaranya adalah *the law of the internet, the law of information and technology, telecommunication law* dan *lex informatica*[123] serta hukum *telematika*. Penggunaan istilah *lex informatica* ini didasarkan pada istilah *lex mercatoria* yang dipergunakan dalam dunia perdagangan.

Meskipun demikian, melihat perkembangan penggunaan internet yang semakin meluas maka apa yang ada di *cyberspace* perlu di atur. Pengaturan

---

122 Mieke Komar Kantaatmaja. *op.cit.* hal. 7
123 *Ibid.* hal. 2

mengenai kegiatan di *cyberspace* ini akan membawa keuntungan sekaligus kerugian.[124] Keuntungannya adalah:

a. merupakan sumber informasi tanpa batas, antara lain bidang *educational websites, newsgroup* dan *discussion group*.
b. Tarifnya relatif murah
c. Membantu di bidang perdagangan karena dapat digunakan untuk virtual mails, pemasaran yang luas, transaksi dengan online secara luas, memberikan pelayanan online, dan memonitor stock (pasar modal).

Kerugian-kerugian yang kemungkinan timbul antara lain:

a. bisa terjadi adanya misinformasi karena fitnah atau karena informasi yang diberikan tidak dapat diverifikasi atau dibuktikan;
b. tidak ada sensor, sehingga mudah untuk penyebaran pornografi atau penyajian informasi yang sensitif;
c. digunakan tindak kejahatan (*cybercrime* atau *cyberattack* melalui virus);
d. sulit dilacak dan dimonitor;
e. pemborosan waktu yang tidak produktif (untuk *chatting*) selama jam kerja
f. keamanan dalam transaksi tidak terjamin kerahasiaannya; dan
g. pelanggaran *privacy*.

Apa yang dikemukakan **Yusril Ihza Mahendra** ini sebenarnya tidak tepat disebut sebagai keuntungan dan kerugian pengaturan kegiatan di *cyberspace*, tetapi lebih tepat keuntungan dan kerugian pemanfaatan internet atau terlibat dalam kegiatan-kegiatan di *cyberspace*. Pengertian yang timbul apabila membaca pendapat **Yusril Ihza Mahendra** ini bisa menyesatkan

---

[124] Yusril Ihza Mahendra, *op.cit.*, hal. 4-5.

mengingat masalah pengaturan berkaitan dengan membuat aturan yang berisi aturan-aturan dan pembatasan-pembatasan.

Ruang lingkup *cyberlaw* menurut **Jonathan Rosenoer** seperti yang termuat dalam bukunya *Cyberlaw, The Law of the Internet* adalah sebagai berikut:[125]

a. Copyright, meliputi, Exclusive Rights, Subject Matter of Copyright, Formalities, Infringement, Sources of Risk, World Wide Web Sites, Hypertext Links, Graphical Elements, E-mail, Postings, Criminal Liability, Fair Use, First Amandement, dan Software Rental.

b. Trademark.

c. Defamation (fitnah atau pencemaran nama baik)

d. Privacy, meliputi Common Law Privacy, Constitutional Law, Anonymity (keadaan anonim pada jaringan internet), dan Technology Expanding Privacy Rights (Pengembangan hak privacy dengan teknologi)

e. Duty of Care, meliputi:

1) *Negligence* (tindakan yang dilakukan di luar kebiasaan tetapi dibenarkan oleh hukum sebagai upaya perlindungan dari resiko kekerasan yang tidak perlu)

2) *Negligent Misstatement* (tindakan yang dilakukan pihak penydeia informasi di interent dengan memberikan informasi yang tidak akurat)

3) *Equipment Malfunctions* (kerusakan teknis dari peralatan, di mana ketidaksiapan untuk mengantisipasi kerusakan teknis tersebut akan menimbulkan tanggung jawab atas *negligence*)

---

[125] Jonathan Rosenoer, *Cyberlaw, The Law of the Internet*, Spring-Verlag, New York, 1997.

4) *Economic loss may not be recoverable* (kerugian yang secara ekonomis tidak dapat digantikan)

5) *Contractual Limitations of Liability* (tanggung jawab keterbatasan kontrak)

f. Criminal Liability, meliputi Computer Fraud and Abuse Act, Wire Fraud, Electronic Communications Privacy Act, Extortion and Threats, Exports, Sexual Exploitation of Children, Obsence and Indecent Telephone Calls, Copyright, Stalking

g. Procedural Issues, meliputi Jurisdiction, Venue dan Conflict of Law

h. Electronic Contracts and Digital Signature meliputi Electronic Agreement Enforceable, Public Key Encryption and Digital Signature

Mieke Komar Kantaatmaja dan **Ahmad M. Ramli** dalam makalah "Kajian dan Evaluasi Hukum Nasional Dalam Pemanfaatan Teknologi Informasi" menunjukkan beberapa permasalahan hukum yang perlu dicermati dalam persiapan regulasi dalam kegiatan di *cyberspace*, yaitu:[126]

a. Aspek hukum perjanjian dan tanda tangan digital

b. Pelanggaran hukum dalam bentuk akses ilegal terhadap jaringan komputer

c. Penyalahgunaan *Password* dalam era ekonomi digital; dan

d. Keterkaitan hak atas kepemilikan intelektual (HAKI) dengan Sistem Informasi (Hak Cipta, Merek, Paten, Informasi Rahasia/Rahasia Dagang/*Trade Secret* dan Disain Industri)

Berdasarkan ruang lingkup yang telah dikemukakan tersebut, maka Tim Pengkajian *Cyberlaw* UNPAD yang kemudian menjadi Tim Perumus RUU

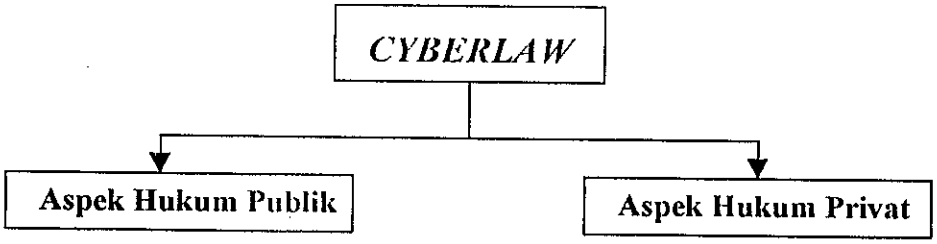
---

126 Mieke Komar Kantaatmaja, *op.cit.*, hal. 4

Teknologi Informasi menyusun langkah-langkah pengkategorian *cyberlaw* sebagai langkah awal dalam upaya untuk melakukan pemahaman dan pengkajian *cyberlaw*. Hasil dari pengkategorian *cyberlaw* yang telah disusun ini terlihat dalam bagan dan gambar di bawah ini.

Bagan 3

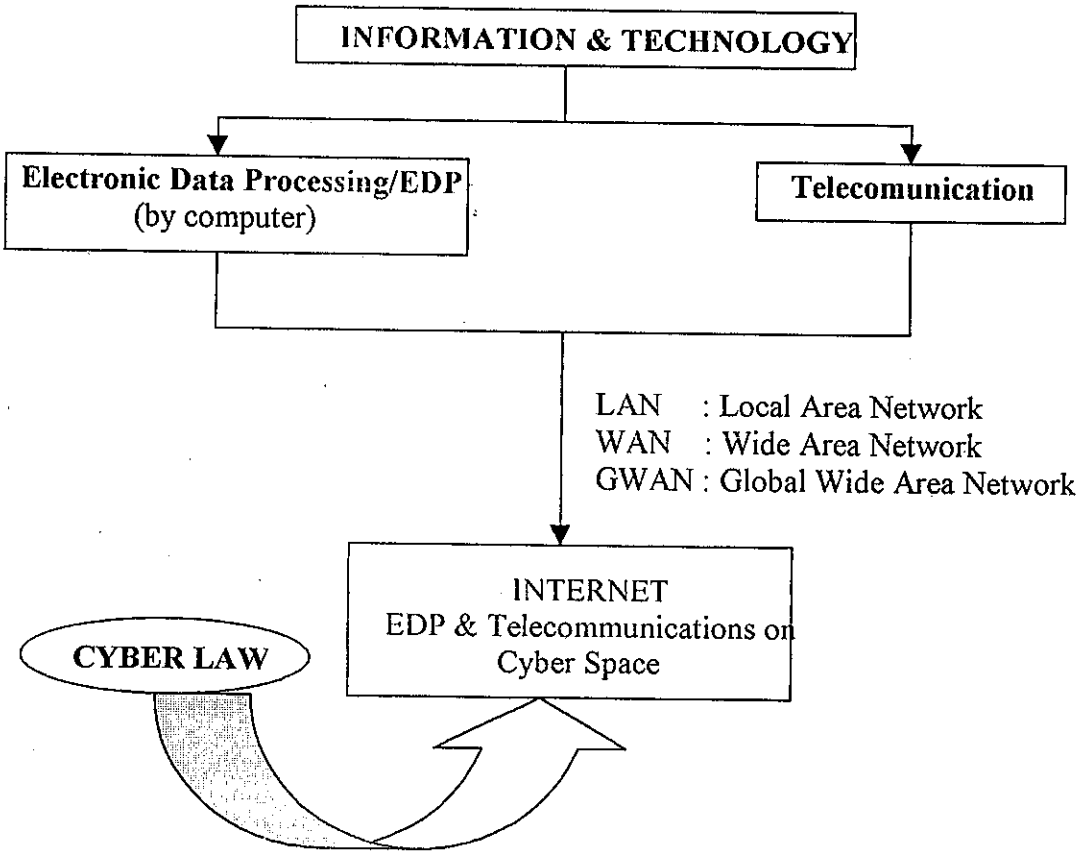
Kategorisasi *Cyberlaw*



Ruang Lingkup *Cyberlaw*	**Aspek-aspek Hukum**
Publik	a. Jurisdiksi dan Kompetensi Badan Peradilan serta aspek pembuktiannya b. Etika kegiatan dalam *Cyberspace* c. Perlindungan konsumen d. Anti Monopoli e. Persaingan Sehat f. Perpajakan g. Regulatory Body h. Perlindungan Electronic Database i. *Cybercrimes*
Privat	a. HAKI (Intellectual Property Rights) b. E-Commerce c. Kontrak dalam Internet (*Cyber* Contract) d. Privacy e. Domain Name f. Asuransi

Bagan 4

Evolusi *Cyberlaw*[127]



Ada dua model yang diusulkan oleh **Mieke** untuk mengatur kegiatan-kegiatan di *cyberspace*, yaitu:[128]

a. Model Ketentuan Payung (*Umbrella Provisions*) sebagai Upaya Harmonisasi Hukum.

   Model ketentuan payung untuk peraturan perundang-undangan yang mengatur kegiatan-kegiatan di *cyberspace*, di satu sisi memilik kebaikan yaitu akan menghaslkan suatu masterpiece dengan memahami sangat beragamnya hal-hal yang perlu diatur, namun di sisi lain kelemahannya

---

127 Sumber dari Danrivanto Budhijanto. *Aspek-aspek Hukum Dalam Perniagaam Secara Elektronik (E-Commerce)*, Makalah pada Seminar Aspek Hukum Transaksi Perdagangan via Internet di Indoensia, FH UNPAD. Bandung, 22 Juli 2000, hal. 3

128 *Ibid*, hal. 7-9

adalah menimbulkan konsekuensi logis untuk mempersialkan dalam waktu yang tidak boleh terlalu lama bagi seluruh rancangan peraturan perundang-undangan yang lebih khusus atau spesifik (baik pada tingkatan yang sederajat maupun pengaturan pelaksanaan teknisnya) agar terhindarkan dari kekosongan hukum.

Model ketentuan payung dapat memuat:

1) materi-materi pokok saja yang perlu diatur dengan memperhatikan semua kepentingan seperti antara lain pelaku uasaha, konseumen, pemerintah, penegak hukum; dan
2) keterkaitan hubungan dengan peraturan perundang-undangan yang telah ada terlebih dahulu dan yang akan datang agar tercipta suatu hubungan sinergis.

b. Model *Triangle Regulations* sebagai upaya mengantisipasi pesatnya laju kegiatan-kegiatan di *Cyberspace*.

Model *Triangle Regulations* merupakan upaya yang lebih menitikberatkan kepada permasalahan manakah yang perlu lebih diberikan prioritas, sehingga mampu secara efisien dan efektif diantisipasi diakrenakan pengaturannya lebih spesifik dan menukik. Jadi tidak perlu adanya pengaturan yang harus memuat seluruh kegiatan-kegiatan di *cyberspace*. Berdasarkan skala prioritas 3 (tiga) regulasi yang dapat disusun terlebih dahulu, yaitu:

1) Pengaturan sehubungan Transaksi Perdagangan Elektronika (*E-Commerce*) atau *On-line Transaction*, yang di dalamnya memuat antara lain tentang *Digital Signature* dan *Certification of Authority*, aspek pembuktian, perlindungan konsumen, anti monopoli dan persaingan sehat, perpajakan, asuransi;

2) Pengaturan sehubungan *Privacy Protection* terhadap pelaku bisnis dan konsumen, yang di dalamnya memuat antara lain perlindungan elelctronic databases, individual/company records; dan

3) Pengaturan sehubungan *Cybercrime*, yang di dalamnya memuat antara lain yurisdiksi dan kompetensi dari badan peradilan terhadap kasus0kasus yang terjadi dalam *cyberspace*, penipuan melalui komputer atau melalui jaringan telekomunikasi, ancaman dan pemerasan, fitnah atau penghujatan (*defamation*), kegiatan transaksi atas substansi yang berbahaya, eksploitasi seksual dari anak-anak, substansi yang tidak layak untuk ditransmisikan.

Dalam kaitannya dengan model-model yang hendak digunakan untuk mengatur kegiatan-kegiatan di *cyberspace*, tampaknya Departemen Perhubungan melalui Direktorat Jenderal Pos dan Telekomunikasi bekerjasama dengan FH UNPAD Bandung menggunakan model payung (*Umbrella Provisions*). Hal ini tercermin dari Naskah Akademik dan Rancangan Undang-undang tentang Teknologi Informasi yang dilakukan dengan pertimbangan-pertimbangan:

a. lebih sejalan dengan sistem hukum Indonesia;

b. lebih efektif dalam penegakannya melalui implementing legislation; dan

c. mengakomodasi kepentingan *ius constitutum* dan *ius contituendum*.

Prinsip pengaturan dalam RUU Teknologi Informasi menggunakan sintesis hukum positif dan *lex informatica*. Strategi pembentukan pengaturan RUU Teknologi Informatika adalah dengan menetapkan prinsip-prinsip

pembentukan dan pengembangan teknologi informasi, yang isinya antara lain sebagai berikut:[129]

a. mengikuti keunikan *cyberspace*;
b. melibatkan unsur-unsur masyarakat, pemerintah, swasta dan profesional serta perguruan tinggi;
c. mendorong peran sektor swasta;
d. mendorong peran masyarakat, swasta, pemerintah, kelompok profesi, dan perguruan tinggi;
e. peran dan tanggung jawab pemerintah terhadap kepentingan publik;
f. aturan hukum yang bersifat preventif, direktif dan futuristik yang tidak bersifat restriktif;
g. mendorong harmonisasi dan uniformitas hukum regional dan internasional; dan
h. melakukan pengkajian terhadap peraturan yang berkaitan langsung atau tidak langsung dengan munculnya persoalan-persoalan hukum akibat perkembangan teknologi informasi.

Departemen Perindustrian dan Perdagangan juga memandang perlu mengatur kegiatan di *cyberspace* khususnya mengenai tanda tangan digital (*Digital Signature*) dalam setiap traksaksi di Internet, nampaknya menggunakan model *Triangle Regulations*. Dalam perumusannya, Departemen Perindustrian dan Perdagangan bekerja sama dengan Fakultas Hukum Universitas Indonesia, Jakarta.

---

[129] Naskah Akademik RUU Teknologi Informasi. UNPAD- DITJEN POSTEL DEPHUB. 2000, hal. 15

Kedua rancangan itu sampai sekarang masih dibuat. Persoalan yang timbul adalah apabila salah satu di antaranya selesai lebih dulu, semisal *Digital Signatur Act*, sedangkan Undang-undang Teknologi Informasi selesai sesudahnya, padahal isi keduanya saling bertentangan (khususnya mengenai Digital Signature itu), bagaimana penyelesaiannya. Tentunya sebelum melangkah lebih lanjut ke arah pembahasan di badan legislatif, harus ada harmonisasi di antara berbagai departemen yang terkait dengan kegiatan *cyberspace* sehingga undang-undang yang terbentuk nantinya tidak menimbulkan kekacauan.

Pengaturan mengenai *cybercrime*[130] (sebagai bagian dari *cyberlaw* dalam pengertian luas), dapat saja dibuat dengan menggunakan model *Umbrella Provisions* ataupun *Triangle Regulation*. Penggunaan salah satu dari kedua model itu tentunya harus memperhatikan perkembangan yang akan terjadi pada teknologi informasi di kemudian hari agar undang-undang yang terbentuk nantinya dapat mencakup perkembangan teknologi informasi yang terjadi setelah undang-undang itu terbentuk.

Seperti halnya pengaturan *cyberlaw* yang menangandung pro kontro mengenai model mana yang hendak dipakai sehingga memunculkan tiga kelompok, demikian pula dengan pengaturan *cybercrime* ini. Dengan menggunakan pendekatan yang ditawarkan oleh **Muladi** ketika membahas mengenai kejahatan komputer, tampaknya model pendekatan ini dapat pula

---

130 Kriminalisasi terhadap *cybercrime* ini sejalan dengan hasil lokakarya Workshop on crimes related to computer networks yang diorganisir oleh UNAFEI selama Kongres PBB X/2000.

digunakan sebagai salah satu pemikiran dan pembentukan undang-undang mengenai *cybercrime*. Pendekatan-pendekatan itu adalah sebagai berikut:[131]

a. Pendekatan pertama dapat disebut sebagai pendekatan global (*global approach*) yang menghendaki adanya pengaturan baru yang bersifat umum terhadap kejahatan komputer yang mencakup pelbagai bentuk perbuatan berupa manipulasi, pengrusakan, pencurian dan penggunaan komputer secara melawan hukum dan tanpa kewenangan (*access to data processing system*). Hal ini nampak misalnya pada *Swedish Data Act 1973;*

b. Pendekatan kedua adalah pendekatan evolusioner (*evolutionary approach*) yang berusaha untuk mengadakan pembaharuan atau amandemen terhadap perumusan kejahatan-kejahatan tradisional dengan menambah objek dan cara-cara dilakukannya kejahatan komputer dalam perumusannya. Penambahan dalam hal ini dapat berarti modifikasi atau berupa suplementasi. Contohnya adalah *Penal Code Amandement Act 1985* di Canada; dan

c. Pendekatan ketiga merupakan kompromi antara pendekatan global dan pendekatan evolusioner dilakukan dengan cara mencantumkan komputer di dalam Kodifikasi Hukum Pidana.

Pendekatan-pendekatan yang ditawarkan **Muladi** itu merupakan pendekatan yang digunakan untuk kejahatan komputer (*computer crime*), sedangkan *computer crime* berbeda dengan *cybercrime*. Istilah *cybercrime* sampai saat ini masih belum ada kesatuan pendapat bahkan tidak ada pengakuan

---

131 Muladi dalam Muladi dan Barda Nawawi Arief, *op.cit*, hal. 31. Bandingkan dengan hasil pengkajian OECD yang juga terdapat dalam buku tersebut hal. 31-32 dan pendapat Atip Latifulhayat pada halaman sebelumnya.

internasional mengenai istilah yang baku, tetapi ada yang menyamakan istilah *cybercrime* dengan *computer crime*. *Computer crime* dan *cybercrime* merupakan dua istilah yang berbeda sebagaimana dikatakan oleh **Nazrul Abdul Manap** sebagai berikut:

> Defined broadly, "computer crime" could reasonably include a wide variety of criminal offences, activities or issues. It also known as a crime committed using a computer as a tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who unauthorisedly transfers a customer's money to a dormant account for his own interest or a person without permission has obtained acces to othrt person's computer directly to download information, which in the first place, are confidential. These situations require direct access by the hacker to the victim's computer. There is no Internet line involved, or only limited networking used such as the Local Area Network (LAN).
> Whereas, *cyber*-crimes are crimes committed virtually through Internet online. This means that the crimes committed could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refer computer crimes as *cybercrime*s or vice versa, since they have same impact in law. [132]

Dengan mendasarkan pada Kongres PBB ke 10 Konggres PBB ke 10 (*Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offender*) di Vienna, istilah yang digunakan untuk *cybercrime* ini adalah *computer related crime* sebagaimana terungkap dari hasil Kongres itu sebagai berikut

> The term "computer-related crime" had been developed to encompass both the entirely new forms of crime that were directed at computers, networks and their users, and the more traditional form of crime that were now being committed with the use or assistance of computer equipment.[133]

---

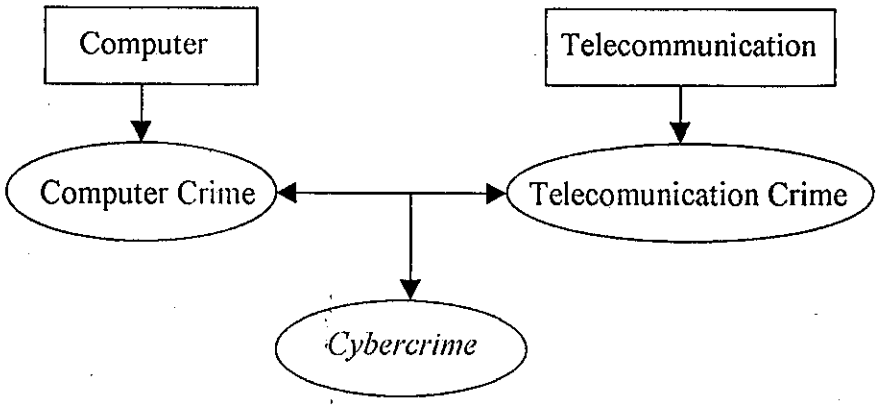
[132] Nazura Abdul Manap, *Cyber*-crimes: *Problems and Solutions Under Malaysian Law*, Makalah pada Seminar Nasional Money Laundering dan *Cybercrime* dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Lab. Hukum Pidana FH Univ. Surabaya, 24 februari 2001, hal. 3

[133] Dokumen A/CONF.187/15, hal. 26

Secara sederhana, penulis membedakan antara *computer crime* dengan *cybercrime* yang didasarkan pada perpaduan antara teknologi komputer dan teknologi telekomunikasi yang menghasilkan Internet, sehingga bagannya adalah sebagai berikut:

Bagan 5

Pembedaan Computer Crime dan *Cybercrime*



Masing-masing penulis mempunyai kategori-kategori sendiri untuk membedakan tipe-tipe dari *cybercrime*. **Nazura Abdul Manap** membedakan tipe-tipe dari *cybercrime* menjadi tiga, yaitu:[134]

a. *cyber-crimes againts property*, meliputi Theft, berupa theft of information, theft of property dan theft of services), Fraud/Cheating, Forgery, dan Mischief.

---

[134] *Ibid*, hal, 3-6. Bandingkan dengan The Broad Spectrum of Threats dari Michael A Vatis yang meliputi Insiders, Hackers, Virus Transmittlers, Criminal Groups, Terrorists, Foreign intelligence services, Information Warfare dalam Michael A. Vatis, Statement of The Record on The National Infrastructure Protection Center, March 1, 2000, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress01.htm Lihat juga Michael A. Vatis, Statemen of the Record on *Cybercrime*, Febnuaty 29, 2000, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress02.htm. Selain hal tersebut, Louis J. Freeh menambahkan hactivism dan distributed denial of service attacks. Lihat lebih jelas pada Louis J. Freeh, Statemen of the Record on *Cybercrime*, Febnuaty 16, 2000, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress03.htm. Bandingkan juga dengan tipe-tipe *cybercrime* dari Gabriole Zeviar-Geese, op.cit.

b. *cyber-crimes againts persons*, meliputi Pornography, *Cyber*-harassment, *Cyber*-stalking dan *Cyber*-trespass. *Cyber*-trespass meliputi Spam email, Hacking a Web page dan Breaking into Personal Computer.

c. *cyber-terrorism.*

Konggres PBB ke 10 (Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offender) di Vienna pada 10-17 April 2000, membagi 2 (dua) sub kategori *cybercrime*, yaitu:[135]

a. *Cybercrime in a narrow sense* (computer crime); any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;

b. *Cybercrime in a broader sense* (computer related crime); any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network

Kategori pertama dari hasil Kongres PBB ini dapat dimasukkan dalam klasifikasi computer crime atau *cybercrime* dalam pengertian yang sempit (meliputi *against a computer system or network*) sedangkan kategori yang kedua diklasifikasikan sebagai *cybercrime* atau *cybercrime* dalam pengertian yang luas (meliputi *by means of a computer system or network* dan *in a computer system or network*).

---

135 Dokumen A/CONF.187/10, hal. 5

Council of Europe dalam *Draft Convention on Cyber-crime* (Draft No. 19) pada Section 1 yang membahas mengenai *Substantive Criminal Law Cyber-crime* menjadi 5 (lima) Tittle atau kategori, yaitu:[136]

Tittle 1 - Offences against the confidentiality, integrity and availability of computer data and systems, yang meliputi:

a. Illegal Acces (article 2) berupa sengaja mengakses atau memasuki sistem komputer tanpa hak (...the access to the whole or any part of a computer system without rights)

b. Illegal Interception (article 3) berupa kesengajaan dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis (...the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, as well as electromagnetic emissions from a computer system carrying sucht computer data)[137]

c. Data Interference (article 4) berupa sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau

---

136. Draft ini dapat dijumpai di http://conventions.coe.int/treaty/en/projects/*cybercrime*.htm, baik versi April 2000, 2 Oktober 2000, 19 November 2000, 22 Desember 2000, 25 Mei 2001 maupun 22 Juni 2001. Explanatory Memorandum dari Draft Convention ini menjelaskan bahwa apa yang diatur dalam konvensi ini merupakan standar minimum untuk delik-delik terkait (a common minimum standard of relevant offences) dan merupakan konsensus minimal (minimum consensus). Penjelasan lebih lanjut mengenai konvensi ini dalam Explanatory Memorandum dapat dilihat pada **Draft 27 of Convention on Cyber-crime and Explantory Memorandum,** May 25, 2001 http://conventions.coe.int/*cybercrime27*.doc maupun dalam Explanatory Memorandum, June 22, 2001 di http://conventions.coe. int/*cybercrimememo-final*..htm. Lihat juga Barda Nawawi Arief. *Antisipasi... op.cit*, hal. 12-13, dan *Kebijakan Kriminalisasi* ..., hal. 8

137. Bandingkan pengertian interception ini dengan pendapat Mark D. Rasch dalam Mark D. Rasch, The Interet and Business: A Lawyer's Guide to the Emerging Legal Issues (Chapter 11 Criminal Law and The Internet), versi elektronik dapat dijumpai di http://cla.org/RuhBook/chp11.htm

penghapusan data komputer (...the damaging, deletion, deterioration, alteration or suppression of computer data without right)

d. System Interference (article 5) berupa sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer (...the serious hindering without right of the functioning of a computer system by inputting (transmitting), damaging, deleting, deteriorating, altering or suppressing computer data)

e. Illegal Devices, meliputi:

1) the production, sale, procurement for use, import, distributin or otherhwise making availabel of:

a) a device, including a computer program, designed or adapted (specifically.primarily/particularly) for the purpose of committing any of the offences established in accordance with article 2-5.

b) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed.

Tittle 2 - Computer-related offences, meliputi

a. Computer-related Forgery, berupa pemalsuan, dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data otentik menjadi tidak otentik dengan maksud digunakan sebagai data otentik (... intionally and without right the input, alteration,

deletion, or suppression of computer data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authetic regardless whether or not the data is directly, readable and intelligible. A party may require by law an intent to defraud or similar dishonest intent, before criminal liability attaches)

b. Computer-related Fraud, berupa penipuan, dengan sengaja atau tanpa hak menyebabkan hilangnya barang atau kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu berfungsinya komputer atau sistem komputer dengan tujuan untuk memperoleh keuntunan ekonomi bagi dirinya (... intention and without right, the causing without right, of a loss of property to another by: any input, alteration, deletion or suppression of computer data; any interference with the functioning of a computer (program) or system, with the intent of procuring, without right, an economic benefit for himself or for another)

Tittle 3 - Content-related offences, meliputi Offences related to child pornography (article 9). Yang termasuk dalam kategori ini adalah delik-delik yang berhubungan dengan pornografi anak, meliputi perbuatan:

a. offering, distributing, transmitting or (otherwise) making available child pornography through a computer system;

b. producing child pornography for the purpose of its distribution through a computer system;

c. possessing child pornography in a computer system or on a data carrier.

Tittle 4 - Copyright and related offences berupa Copyright and related offences (article 10)

Tittle 5 - Ancillary liability and sanctions, meliputi

a. Attemps and aiding and abetting (article 11)

b. Corporate liability (article 12)

c. Sanctions and measures (article 13)

Singapura dengan *The Computer Misuse Act* (CMA) yang telah diundangkan pada tahun 1993 dan kemudian diamandemen pada tahun 1998 mengkategorikan *cybercrime* menjadi beberapa beberapa section, yaitu:[138]

a. any person who gains unauthorized access to any program or data held in any computer;

b. any person who accesses a computer with intent to commit or facilitate the commission of an offence involving property, fraud, dishonesty, or which causes bodily harm;

c. any person who causes an unauthorized modification of the contents of any computer;

d. any person who accesses a computer for unauthorized use or interception of any computer service.

---

138 The Computer Misuse Act 1998, lihat juga Acdit Abdullah, *Cybercrime in Singapore (and Money-Laundering)*, Makalah pada Seminar Nasional Money Laundering dan *Cyber* Crime dalam Perspektif Penegakan Hukum di Indonesia, Lab Hukum Pidana, FH Univ. Surabaya, 24 Februari 2001; dan Muladi, op.cit, hal. 8.

Kategori a dapat diklasifikasikan dalam *Unauthorised access*, di atur dalam section 3 CMA, kategori b masuk dalam kualifikasi *Access to commit another offence* diatur dalam section 4 CMA. *Unauthorized modification of computer material* merupakan kualifikasi dari kategori dari c yang diatur dalam section 5 CMA, sedangkan kategori c termasuk dalam kualifikasi *Unauthorized use and interception,* diatur dalam section 6.

India dengan *The Information Technology Act 1999*[139] pada Chapter IX mengenai *Penalties and Adjudication*, Pasal 43 menentukan bahwa seseorang dihukum untuk kerusakan pada komputer atau sistem komputer dan lain-lain jika orang tanpa ijin dari pemiliknya atau setiap orang yang menyerang komputer, sistem komputer atau komputer jaringan:

a. accesses or secures access to such computer, computer system or computer network;
b. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d. damage or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
e. disrupts or causes disruption of any computer, computer system or computer network;

---

139 Dapat dilihat pada http://www.cyberlawindia.com/itbill.html

f. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

g. provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, roles or regulation made thereunder;

h. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network,

he shall be liable to pay damages by way of compensation not exceeding ten lakh rupees to the person so affected.

Malaysia dengan *The Computer Crime Act 1997* juga telah mengatur masalah *cybercrime* ini dalam beberapa pasalnya. The Computer Crime Act ini membagi tiga serangan pokok dalam *cybercrime*, yaitu:[140]

a. Unauthorized access to computer materials or also known as hacking (Section 3). Section 3 (1) menentukan menghukum orang yang menyerang, jika:

   1) he causes a computer to perform anny function with intent to secure access to any program or data held in any computer;

   2) the access he intends to secure is unauthorized, and

   3) he knows at the time when he causes the computer to perform the function that is the case.

b. Unauthorized access with intent to commit or facilitate commission of futher offence or also known as cracking (Section 4)

---

[140] Lihat lebih lanjut pasal-pasal mengenai *cybercrime* dalam The Computer Crime Act 1997 dan lihat juta Nazura Abdul Manap, op.cit, hal. 11.

c. Unauthorized modifications of the contents of any computer (Section 5).

Indonesia meskipun saat ini masih membahas rancangan undang-undang mengenai *cybercrime* ini. Model yang digunakan adalah *Umbrella provision* sehingga ketentuan *cybercrime* tidak dalam perundang-undangan tersendiri tetapi diatur secara umum dalam RUU Teknologi Informasi. Pasal-pasal yang menyangkut ketentuan pidana adalah sebagai berikut:[141]

a. dengan sengaja dan melawan hukum atau tanpa hak mengakses data komputer atau program komputer atau jaringan komputer dengan atau tanpa merusak sistem keamanan (Pasal 31);
b. dengan sengaja dan melawan hukum:
   1) menahan atau mengintersepsi pengiriman data komputer dari atau ke dalam sistem komputer atau jaringan komputer untuk menguntungkan diri sendiri atau orang lain (Pasal 32 ayat (1))
   2) atau tanpa hak mengintersepsi pengiriman data komputer sehingga menghambat komunikasi dalam sistem komputer atau jaringan komputer atau sistem telekomunikasi (Pasal 32 ayat (2))
c. dengan sengaja dan melawan hukum atau tanpa hak mengubah, menghapus atau merusak data komputer atau program komputer atau data elektronik lainnya (Pasal 33 ayat (1))
d. dengan sengaja dan melawan hukum atau tanpa hak memasukkan, mengubah atau menghapus data komputer atau data elektronik lainnya yang mengakibatkan terganggunya fungsi sistem komputer (Pasal 33 ayat (2))

---

[141] Draft I RUU Teknologi Informasi disusun oleh FH UNPAD bekerja sama dengan Ditjen Pos dan Telekomunikasi, 2001. Lihat juga Naskah Akademik RUU Teknologi Informasi, UNPAD-Ditjen Postel Departemen Perhubungan, 2000.

e. dengan sengaja dan melawan hukum atau tanpa hak menggunakan, mengubah, menambah atau menghapus data komputer atau programkomputer atau jaringan komputer atau data elektronik lainnya atau melakukan perbuatan lain yangmengakibatkan timbulnya kerugian ekonomis bagi pihak lain (Pasal 34)

f. dengan sengaja dan melawan hukum atau tanpa hak mengubah, menambah atau menghapus data komputer atau program komputer atau data elektronik lainnya atau melakukan perbuatan lain yang mengakibatkan terjadinya pemalsuan data (Pasal 35)

g. dengan sengaja dan melawan hukum atau tanpa hak memproduksi, menjual, mengimpor atau mendistribusikan peralatan sistem komputer termasuk program komputer, sandi akses, kode akses komputer atau data sejenis untuk melakukan tindak pidana sebagaimana di atur dalam Pasal 30 sampai Pasal 35 (Pasal 36 ayat (1))

h. dengan sengaja dan melawan hukum atau tanpa hak membuat menyediakan atau mengirimkan, mendistribusikan data atau tulisan atau gambar atau rekaman yang isinya melanggar kesusilaan dengan menggunakan sistem komputer atau jaringan komputer (Pasal 37 ayat (1))

i. dengan sengaja dan melawan hukum atau tanpa hak melakukan tindak pidana sebagaimana dimaksud dalam Pasal 37 ayat (1) yang objeknya adalah anak di bawah umur atau menggunakan sistem komputer atau jaringankomputer sebagai sarana untuk melakukan tindak pidana kesusilaan terhadap anak di bawah umur (Pasal 37 ayat (2))

j. dengan sengaja dan melawan hukum atau tanpa hak menggunakan jaringan komputer mengirimkan data atau tulisan atau gambar atau rekaman yang isinya mengancam orang lain sehingga mengakibatkan terganggunya ketentraman orang tersebut (Pasal 38)

k. dengan sengaja dan melawan hukum atau tanpa hak dengan menggunakan jaringan komputer mengirimkan data atau tulisan atau gambar atau rekaman yang isinya menyerang kehormatan atau nama baik orang lain (Pasal 39)

l. dengan maksud menguntungkan diri sendiri atau orang lain dan melawan hukum:

   1) membuat, menyediakan atau mengirimkan, data atau tulisan atau gambar atau rekaman yang bertentangan dengan kewajiban selaku produsen dalam transaksi perdagangan melalui jaringan komputer (Pasal 40 ayat (1))

   2) menggunakan identitas palsu atau data yang bukan miliknya dalam transaksi perdagangan melalui internet atau jaringan komputer agar orang lain menyerahkan barang sesuatu kepadanya (Pasal 40 ayat (2))

m. dengan sengaja dan secara melawan hukum atau tanpa hak memperbanyak atau mendistribusikan hak cipta milik orang lain melalui jaringankomputer, seolah-olah sebagai miliknya sendiri untuk kepentingan komersial (Pasal 41 ayat (1))

n. dengan maksud untuk menguntungkan diri sendiri atau orang lain dan melawan hukum atau tanpa hak menyebarluaskan program komputer atau software lainnya sehingga dapat digunakan oleh orang lain (Pasal 40 ayat 92))

Dari ketentuan yang terdapat dalam RUU Teknologi Informasi terlihat bahwa ruang lingkup yang telah dikemukakan ternyata tidak berbeda jauh dengan apa yang telah diatur dalam perundang-undangan di negara lain. Apa yang telah dikemukakan dalam RUU Teknologi itu belum termasuk bentuk *cybercrime* yang lain seperti *cyber*terorism, *cyberstalking* dan lain-lain.

Khusus mengenai hacking, selain diatur secara tersendiri dalam Pasal 31, sebenarnya pasal-pasal lain dapat juga dikenakan pasal hacking tersebut karena hacking merupakan *first crime*. Bagaimana dapat mengubah, menghapus atau menambah data komputer apabila dia tidak bisa masuk dalam sistem jaringan komputer yang menjadi korban, sedangkan masuk ke dalam sistem jaringan komputer merupakan langkah *hacking* yang kedua setelah sebelumnya melakukan observasi terhadap sistem operasi yang dipakai.

Selain melakukan upaya dengan mengkriminalisasikan kegiatan di *cyberspace* dengan pendekatan global, Indonesia juga sedang melakukan pendekatan evolusioner untuk mengatur kegiatan di *cyberspace* dengan memperluas pengertian-pengertian yang terdapat dalam RUU KUHP 1999/2000. Di katakan evolusioner karena dari RUU KUHP yang ada sebelumnya tidak memperluas pengertian-pengertian yang terkait kegiatan-kegiatan di *cyberspace*. Menurut **Barda Nawawi Arief**, kebijakan yang ditempuh sementara dalam Konsep 2000 yang berkaitan dengan kegiatan di *cyberspace* adalah sebagai berikut:[142]

a. Dalam Buku I (Ketentuan Umum) dibuat ketentuan mengenai:

---

[142] Barda Nawawi Arief, *Antisipasi Penanggulangan Cybercrime .... op.cit.*, hal. 13-14. Lihat juga RUU KUHP, Direktorat Perundang-undangan, Ditjen Hukum dan Perundang-undangan, Departemen Hukum dan Perundang-undangan, 1999-2000.

- ☑ Pengertian "barang" (Pasal 174) yang di dalamnya termasuk benda tidak berwujud berupa data dan program komputer, jasa telepon atau telekomunikasi atau jasa komputer;
- ☑ Pengertian "anak kunci" (Pasal 178) yang di dalamnya termasuk kode rahasia, kunci masuk komputer, kartu magnetik, signal yang telah diprogram untuk membuka sesuatu.

  Maksud dari anak kunci ini kemungkinan besar adalah password atau kode-kode tertentu seperti privat atau public key infrastructure.
- ☑ Pengertian "surat" (Pasal 188) termasuk data tertulis atau tersimpan dalam disket, pita magnetik, media penyimpanan komputer atau penyimanan data elektronik lainnya.
- ☑ Pengertian "ruang" (Pasal 189) termasuk bentangan atau terminal komputer yang dapat diakses dengan cara-cara tertentu.

  Maksud dari ruang ini kemungkinan termasuk pula dunia maya atau mayantara atau *cyberspace* atau virtual reality.
- ☑ Pengertian "masuk" (Pasal 190) termasuk mengakses komputer atau masuk ke dalam sistem komputer.

  Maksud pengertian "masuk" dalam pasal ini menurut penulis bukanlah masuk ke dalam komputer atau sistem komputer (karena seperangkat atau sebuah komputer atau beberapa komputer yang terhubung seperti LAN sudah merupakan sistem) melainkan masuk ke dalam sistem jaringan informasi global yang disebut internet dan kemudian baru masuk ke sebuah situs atau website yang di dalamnya berupa server dan

komputer yang termasuk dalam pengelolaan situs. Jadi ada dua pengertian masuk, yaitu masuk ke internet dan masuk ke situs.

- ☑ Pengertian "jaringan telepon" (Pasal 191) termasuk jaringan komputer atau sistem komunikasi komputer.

b. Dalam Buku II

Dengan dibuatnya ketentuan seperti di atas, maka Konsep tidak atau belum membuat delik khusus untuk *cybercrime* atau computer-related crime. Konsep juga mengubah perumusan delik atau menambah delik-delik baru yang berkaitan dengan kemajuan teknologi, dengan harapan dapat menjaring kasus-kasus *cybercrime*, antara lain:

- ☑ Menyadap pembicaraan di ruangan tertutup dengan alat bantu teknis (Pasal 263)
- ☑ Memasang alat bantu teknis untuk tujuan mendengar atau merekam pembicaraan (Pasal 264)
- ☑ Merekam (memiliki atau menyiarkan) gambar dengan alat bantu teknis di ruangan tidak untuk umum (Pasal 266)
- ☑ Merusak atau membuat tidak dapat dipakai bangunan untuk sarana atau prasarana pelayanan umum seperti bangunan telekomunikasi atau komunikasi lewat satelit atau komunikasi jarak jauh (Pasal 546)
- ☑ Pencucian uang atau *money laundering* (Pasal 641-642)

Dari uraian di atas dapat diketahui bahwa ada dua usaha yang dilakukan oleh pemerintah dalam menanggulangi *cybercrime* yang menggunakan sarana penal, yaitu dengan membuat undang-undang mengenai teknologi informasi atau telematika atau apapun namanya dan upaya memperluas pengaturan-

pengaturan *cyberspace* dalam RUU KUHP dengan memperluas beberapa pengertian yang berkaitan dengan kegiatan di *cyberspace*. Tetapi sebelum sampai kepada bentuk pengaturannya, ada persoalan yang mesti dipecahkan. Persoalan tersebut adalah:

a. Usaha membuat undang-undang yang mengatur mengenai kegiatan di *cyberspace* atau *cyberlaw* memang perlu. Mengingat luas lingkup pengaturan dalam *cyberspace* maka undang-undang ini akan menjadi semacam payung untuk semua bentuk perundang-undangan yang mengatur berbagai jenis kegiatan di *cyberspace*. Persoalan yang muncul adalah pada setiap aktivitas di *cyberspace* seperti *e-commerce* selalu mengandung unsur pidana. Apakah pengaturan pidana nantinya ada di *cyberlaw*-nya atau misalnya digabung dengan pengaturan e-commerce, atau membuat peraturan tersendiri mengenai *cybercrime*. Jika pengaturan yang digunakan adalah model *umbrella provision*, maka ketentuan mengenai *cybercrime* hanya akan menjadi salah satu bagian dari *cyberlaw* untuk seluruh kegiatan yang ada di *cyberspace*. Jika yang digunakan adalah *triangle regulation*, maka setiap perundang-undang yang menyangkut berbagai kegiatan di *cyberspace* mengandung di dalamnya pasal-pasal pidana. Hal ini akan menjadi masalah jika tidak ada harmonisasi atau jika salah satu dari kegiatan di *cyberspace* telah maju dibandingkan yang lain, maka ketentuan pidana dari masing-masing kegiatan akan berbeda. Jika yang dilakukan adalah membuat undang-undang *cybercrime* secara tersendiri, maka tentunya hal ini di luar kebiasaan, artinya selama ini peraturan yang mengatur suatu kegiatan atau aktivitas selalu mencantumkan ketentuan pidana sebagai salah

satu bagiannya dan jikapun ada yang secara khusus mengatur mengenai ketentuan pidana secara keseluruhan adalah KUHP, lalu bagaimana kedudukan KUHP yang ada.

b. Ada juga usaha untuk memperluas peraturan pidana (KUHP) yang ada dengan penafsiran, meskipun penafsiran itu terkadang tidak tepat karena perbedaan paradigma antara undang-undang itu dengan intisari dari peristiwa yang terjadi di *cyberspace*. Usaha lain adalah dengan menyiapkan KUHP mendatang dengan memperluas pengertian-pengertian mengenai berbagai hal agar dapat menjangkau kegiatan di *cyberspace*. Usaha semacam ini sebenarnya hanya melegalisasi atau menampung apa yang telah dilakukan oleh BPHN, padahal kegiatan di *cyberspace* terus berkembang dan berubah, kemudian yang menjadi pertanyaan adalah apakah perluasan pengertian itu akan mencakup perkembangan yang terjadi di *cyberspace* di masa yang akan datang atau hanya mencakup kegiatan di *cyberspace* seperti yang terjadi sekarang ini. Jika keadaannya seperti yang terakhir maka KUHP yang akan datang tidak akan beda dengan KUHP yang sekarang dan salah satu alternatif untuk menangani kejadian yang kemudian berkembang adalah seperti apa yang dilakukan oleh BPHN yaitu dengan penafsiran.

Terhadap kedua persoalan itu maka penulis memberikan beberapa alternatif pemecahan dalam rangka pencegahan dan penanggulangan kejahatan dengan sarana penal. Alternatif-alternatif tersebut adalah sebagai berikut:

a. Jika yang hendak dibuat adalah *cyberlaw* sebagai umbrella provision, maka langkah yang harus diambil adalah membuat ketentuan *cybercrime* yang dapat mencakup semua kegiatan di *cyberspace*. Mengingat ketentuan ini

merupakan ketentuan pidana khusus, maka aturan main yang bersangkutan dengan prinsip atau asas-asas umum harus diatur secara tersendiri. Jika ketentuan *cybercrime* tidak mengatur secara tersendiri mengenai prinsip atau asas-asas umum itu maka apakah ketentuan umum dalam Buku I KUHP dapat diberlakukan padanya, mengingat sifat yang berbeda dari virtual reality dan real life. Ini berarti ada pemisahan antara ketentuan pidana yang berlaku untuk kegiatan di *cyberspace* atau dunia maya (KUHP *Cyberspace*) dan ketentuan pidana yang mengatur kegiatan di kehidupan nyata (KUHP seperti yang sekarang ada).

b. Jika yang ingin dikembangkan adalah KUHP-nya (yang sekarang dilakukan dengan penafsiran) atau dalam KUHP mendatang dengan memperluas penafsiran yang dapat menjangkau kegiatan di *cyberspace*, maka ketentuan pidana di *cyberlaw* atau peraturan tersendiri mengenai *cybercrime* tidak diperlukan karena KUHP merupakan kodifikasi dari hukum pidana. Jika model ini yang diambil/dianut maka harus dikembangkan langkah-langkah untuk menyesuaikan dengan perkembangan *cyberspace* yang begitu cepat yaitu dengan melakukan amandemen. Dengan demikian antara dunia nyata (real life) dan dunia maya hanya ada satu ketentuan pidana yang mengatur kegiatan di kedua dunia tersebut.

Berkaitan dengan penggunaan hukum pidana ini, **Nigel Walker** mensyaratkan adanya enam prinsip yang harus diperhatikan oleh pembentuk undang-undang, yaitu:[143]

---

[143] Nigel Walker dalam Muladi, *Proyeksi Hukum Pidana Materiil Indonesia di Masa Mendatang*, Pidato Pengukuhan Guru Besar Universitas Diponegoro, Semarang, 1990, hal. 7 dan 28.

a. hukum pidana tidak digunakan semata-mata untuk tujuan pembalasan;
b. tindak pidana yang dilakukan harus menimbulkan kerugian dan korban yang jelas;
c. hukum pidana tidak digunakan apabila masih ada cara lain yang lebih baik dan lebih prima;
d. kerugian yang ditimbulkan karena pemidanaan harus lebih kecil daripada akibat tindak pidana;
e. harus mendapat dukungan masyarakat; dan
f. harus dapat diterapkan dengan efektif.

Perlu diperhatikan pula pandangan Sudarto mengenai penggunaan hukum pidana dan kriminalisasi suatu perbuatan menjadi tindak pidana, yaitu sebagai berikut:[144]

a. Hukum pidana harus digunakan untuk mewujudkan masyarakat adil dan makmur, merata materiil dan spirituil. Hukum pidana bertugas untuk menanggulangi kejahatan dan juga pengugeran terhadap tindakan penanggulangan itu sendiri untuk kesejahteraan masyarakat atau untuk pengayoman masyarakat.
b. Hukum pidana digunakan untuk mencegah atau menanggulangi perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian pada masyarakat.
c. Penggunaan sarana hukum pidana dengan sanksi yang negatif perlu disertai dengan perhitungan biaya yang harus dikeluarkan dan hasil yang diharapkan akan dicapai (*cost and benefit principle*).

---

[144] Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1986, hal. 36-40

Dalam pembuatan peraturan hukum pidana perlu diperhatikan kemampuan daya kerja dari badan-badan tersebut, jangan sampai ada kelampauan beban tugas atau *over belasting*.

Untuk mengatur suatu perbuatan (termasuk di *cyberspace*) yang hendak dikriminalisasikan, OECD berusahan membuat bentuk model law yang diharapkan dapat dijadikan pedoman oleh pelbagai negara untuk mengatur *criminal privacy protection*. Hal ini dilakukan untuk menghindarkan terjadinya *under and over criminalization*. Asas-asas ini mencakup:[145]

a. Berdasarkan atas kenyataan, bahwa perlindungan rahasia pribadi lebih bersifat perdata dan administrasi, maka sudah selayaknya apabila hukum pidana digunakan sebagai sarana terakhir (*ultima ratio principle*)
b. Masing-masing ketentuan pidana yang akan dibuat harus secara tepat dan teliti menggambarkan perbuatan yang dilarang dan harus dihindarkan perumusan yang bersifat samar dan umum (*precision principle*)
c. Perbuatan yang dikriminalisasikan harus digambarkan secara jelas dalam ketentuan hukum pidana (*clearness principle*)
d. Perumusan pelanggaran terhadap kerahasiaan pribadi harus dilakukan dengan menghindarkan perumusan yang bersifat global. Asas culpabilitas menghendaki adanya pertimbangan terhadap keraguan yang disebabkan karena kepentingan yang dirusakkan, perbuatan-perbuatan yang dilakukan, status pelaku tindak pidana dan sebagainya (*principle of differentiation*)
e. Perbuatan yang dilakukan dengan kesengajaan. Kriminalisasi perbuatan-perbuatan cula mensyaratkan pembenaran khusus (*principle of intents*)

---

145 Model Law OECD sebagaimana di kutip Muladi dalam Muladi dan Barda Nawawi Arief, *op.cit*, hal. 34.

f. Pemidanaan hanya dilakukan atas permintaan si korban (*principle of victim application*).

Membuat regulasi (khususnya hukum pidana mengenai hacking yang menjadi pokok bahasan dalam tesis ini) terhadap suatu aktivitas yang sangat kompleks apalagi dalam kaitannya dengan teknologi informasi (di mana Indonesia dalam hal teknisnya masih tertinggal) bukanlah suatu pekerjaan yang mudah. Untuk mengadakan perubahan hukum pidana yang ada, orang tidak boleh bertindak begitu saja tanpa ada penelitian yang cukup mendalam sebelumnya. Untuk itu diperlukan fakta-fakta dan data statistik yang dapat menjadi dasar penentuan sesuatu keputusan kehendak dari pembentuk undang-undang yang berupa suatu peraturan.[146]

Selain adanya pengkajian terhadap masalah yang hendak dikriminalisasi (yang hasilnya berupa *academic draft*), persyaratan lain yang perlu diperhatikan adalah kerugian atau korban baik aktuil maupun potensial yang signifikan dengan perbuatan tersebut, tidak boleh bersifat ad hoc, ketentuan hukum pidana harus dapat dioperasionalkan (*enforceable*) dan adanya keyakinan bahwa tidak ada sarana lain yang dapat mengatasinya (*ultima ratio principle*). Syarat terakhir sangat penting untuk menghindarkan adanya kondisi yang disebut kriminalisasi yang berkelebihan (*overcriminalization*) atau inflasi pengaturan yang mengakibatkan turunya nilai hukum pidana di masyarakat, sehingga

---

146 Sudarto, *op.cit.*, hal. 97. Hal senada juga diungkapkan oleh Muladi dalam konteks pembahasan mengenai pengaturan *cybercrime*. Muladi menegaskan adanya persyaratan academic draft yang secara komprehensif dapat meyakinkan pengundang-undang tentang betapa pentingnya proses tersebut atas dasar kebutuhan hukum yang berkaitan dengan substansinya. Muladi, *Prosepek Pengaturan Cybercrime di Indonesia*, Makalah pada Seminar Nasional Money Laundering dan *Cybercrime* dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Lab. Hukum Pidana FH Univ. Surabaya, 24 Februari 2001, hal. 1

bersifat counter productive. Hal ini antara lain dalam bentuk terhambatnya kreativitas pengembangan teknologi informatika. Belum lagi persyaratan teknis yaitu keharusan untuk memenuhi asas *lex certa* bahwa perumusan harus jelas sehingga dapat dipercaya.[147]

Sedemikian kompleksnya sebuah undang-undang hendak dibuat, tentunya membuat kita harus berfikir tentang alternatif apa yang bisa dilakukan untuk mempercepat atau paling tidak menanggulangi *cybercrime* khususnya hacking ini. Meskipin hukum pidana merupakan alat terakhir (*ultimim remidium*) tetapi hukum pidana bukanlah alat yang ampuh karena penanggulangan kejahatan dengan hukum pidana hanya merupakan pengobatan simptomatik.

Meskipun hukum pidana digunakan sebagai ultimum remidium atau alat terakhir apabila bidang hukum yang lain tidak dapat mengatasinya, tetapi harus disadari bahwa hukum pidana memiliki keterbatasan kemampuan dalam menanggulangi kejahatan. Keterbatasan-keterbatasan tersebut sebagaimana dikemukakan oleh **Barda Nawawi Arief** adalah sebagai berikut:[148]

a. sebab-sebab kejahatan yang demikian kompleks berada di luar jangkauan hukum pidana;
b. hukum pidana hanya merupakan bagian kecil (sub sistem) dari sarana kontrol sosial yang tidak mungkin mengatasi masalah kejahatan sebagai masalah kemanusiaan dan kemasyarakatan yang sangat kompleks (sebagai

---

147 Muladi, *ibid.*

148 Barda Nawawi Arief, Baras-batas Kemampuan Hukum Pidana Dalam Penanggulangan Kejahatan, dalam Barda Nawawi Arief, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Citra Aditya Bakti, Bandung, 1998, hal. 46-47

masalah sosio-psikologis, sosio-politik, sosio-ekonomi, sosio-kultural dan sebagainya);

c. penggunaan hukum pidana dalammenanggulangi kejahatan hanya merupakan "kurieren am symptom", oleh karena itu hukum pidana hanya merupakan "pengobatan simptomatik" dan bukan "pengobatan kausatif";
d. sanksi hukum pidana merupakan "remedium" yang mengandung sifat kontradiktif/paradoksal dan mengandung unsur-unsur serta efek sampingan yang negatif;
e. sistem pemidanaan bersifat fragmentair dan individual/personal, tidak bersifat struktural/fungsional;
f. keterbatasan jenis sanksi pidana dan sistem perumusan sanksi pidana yang bersifat kaku dan imperatif;
g. bekerjanya/berfungsinya hukum pidana memerlukan sarana pendukung yang lebih bervariasi dan lebih menuntut "biaya tinggi".

Senada dengan keterbatasan sarana penal dalam penanggulanan kejahatan khususnya *cybercrime* seperti tersebut di atas, Kongres PBB X/2000 juga mengakui penanggulangan *cybercrime* ini tidak mudah. Kesulitan-kesulitan yang ditemui dalam penanggulangan dengan sarana penal ini antara lain:[149]

a. Criminal behaviour can take place in an electronic environment. Investigation of *cybercrimes*, that is, any crime committed in an electronic network, requires particular expertise, investigating procedures and legal powers that may not be available to law enforcement authorities of the State concerned;
b. Internatioanl computer networks, such as the Internet, are open environments that enable users to act beyond the borders of the State

[149] Dokumen PBB A.CONF.187/10 hal. 3

in which they are located. However, investigative efforts of law enforcement authorities in general should be restricted to the territory of their own State. This means that crime control in open computer networks requires intensified international cooperation;

c. The open structures of international computer networks offer users the opportunity to choose the legal environment that best suits their purpose. Use may choose a country where certain forms of behaviour capable of being criminalized. This can attract criminal activity by persons from other States where such activities are criminal under their domestic law. The occurrence of "data havens" -- State where reducing or preventing the misuse of computer networks is not a priority, or where no effective procedural laws have been developed -- may impede the efforts of other countries to control crime in computer networks.

Keterbatasan-keterbatasan hukum pidana inilah yang tampaknya dialami oleh Polri yang menggunakan hukum pidana sebagai landasan kerjanya. Sebab kejahatan yang kompleks ini terlambat diantisipasi oleh Polri sehingga ketika terjadi kasus yang berdimensi baru mereka tidak secara tanggap menanganinya. Untuk itu pencegahan kejahatan tidak melulu harus menggunakan hukum pidana. Agar penanggulangan *cybercrime* ini dapat dilakukan secara menyeluruh maka tidak hanya pendekatan yuridis atau penal yang dilakukan, tetapi dapat juga dilakukan dengan pendekatan non penal.

Dalam konteks *cybercrime* ini erat hubungannya dengan teknologi, khususnya teknologi komputer dan telekomunikasi sehingga pencegahan *cybercrime* dapat digunakan melalui saluran teknologi atau disebut juga *techno-prevention*. Langkah ini sesuai dengan apa yang telah diungkapkan oleh International Information Industri Congress (IIIC) sebagai berikut: [150]

The IIIC recognizes that government action and international treaties to harmonize laws and coordinate legal procedures are key in the fight cyber crime, but warns that these should not be relied upon as the only

[150] Dikutip dari Barda Nawawi Arief, *ibid*, hal. 5

> instruments. Cyber crime is enabled by technology and requires as healty reliance on technology for its solution.

Pendekatan teknologi ini merupakan sub sistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau kultural ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cybercrime* dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan.. Pentinganya pendekatan budaya ini, khususnya upaya mengembangkan kode etik dan perilaku (*code of behaviour and ethics*) terungkap juga dalam pernyataan IIIC sebagai berikut:[151]

> IIIC members are also committed to participate in the development of code behaviour and ethics around computer and Internet use, and in campaigns for the need for ethical and responsible online behaviour. Given the international reach of Internet crime, computer and Internet users around the world must be made aware of the need for high standards of conduct in *cyberspace*.

Ketidaksiapan hukum dan Polri dalam menanggulangi *cybercrime* ini menyebabkan pencegahan dengan menggunakan teknologi dan budaya menjadi alat yang ampuh. Hal ini terungkap dari korban hacking yang merasa nyaman dengan pendekatan teknologi untuk menanggulangi *cybercrime*. Ketika situs mereka dirusak, mereka menggunakan teknologi untuk memperbaikinya dan mengantisipasinya dengan memasang sistem pengamanan yang ketat untuk mencegah serangan berikutnya dari cracker yang tidak bertanggung jawab. Meskipun sistem pengamanan yang baik itu mahal, mereka berani melakukakan

---

151 *Ibid.*

untuk melindungi data-data penting dan pelayanan kepada masyarakat. Dengan nada yang hampir sama dengan pernyataan di atas, **Michael A. Vatis** melihat ada dua kunci dalam pencegahan dan penanggulangan *cybercrime*, yaitu[152]

a. The first is that our role in combating cyber crime is essentially two - fold:
   1) preventing cyber attacks before they occur or limiting their scope by disseminating warnings and advisories about threats so that potential victims can protect themselves, and
   2) responding to attacks that do occur by investigating and identifying the perpetrator.
b. Second, in gathering information as part of our warning and response missions, we rigorously adhere to constitutional and statutory requirements.

Tidak hanya pendekatan penal dan non penal yang diperlukan dalam penanggulangan *cybercrime* ini, mengingat sifat *cybercrime* yang dapat dilakukan oleh orang dengan melalui batas negara maka perlu dilakukan kerjasama dengan negara lain. Bentuk kerjasama ini dapat berupa kerjasama ekstradisi maupun harmonisasi hukum pidana substantif sebagaimana terungkap dari hasil Kongres X/2000, "*The harmonization of substantive criminal law with regard to cyber crimes is essential if international cooperation is to be achieved between law enforcement and the judicial authorities of different States.*"[153]

Berkaitan dengan *cybercrime* dan masalah jurisdiksi peradilan, di mana hukum suatu negara tidak dapat menjangkau pelaku kejahatan di luar negaranya, maka menurut **Aedit Abdullah** solusinya adalah *Co-operation*

---

152 Michael A. Vatis, Statemen of the Record on *Cybercrime*, Februaty 29, 2000, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress02.htm

153 Dengan mendasarkan pada pengalaman European Council dalam menyusun kebijakan kriminalisasi di bidang cybercrime ini, Barda Nawawi Arief menyarakan dalam penyusunan tindak pidana (kebijakan kriminalisasi) dalam RUU Teknologi Informasi seyogyanya ditempuh terlebih dahulu kajian mengenai, pertama harmonisasi materi/substansi tindak pidana dan kedua harmonisasi kebijakan formulasi tindak pidana. Barda Nawawi Areif, *Kebijakan Kriminalisasi ....., op.cit*, hal. 6

between Agencies dan Model-Law Recommendations.[154] Langkah seperti ini sebenarnya juga dianjurkan oleh *Council Europe*.

Satu langkah lagi agar penanggulangan *cybercrime* ini dapat dilakukan dengan baik maka perlu dilakukan kerjasama dengan *Internet Service Provider* (ISP) atau penyedia jasa internet. Meskipun ISP hanya berkaitan dengan layanan sambungan atau akses Internet, tetapi ISP memiliki catatan mengenai keluar atau masuknya seorang pengakses, sehingga ia sebenarnya dapat mengidentifikasikan siapa yang melakukan kejahatan dengan melihat log file yang ada. Pemanfaatan ISP dalam penanganan dan penanggulangan *cybercrime* ini sesuai dengan hasil Kongres PBB X/2000 yaitu:

> This means that Internet Providers generally have no legal obligation to monitor or possibly block traffic that is transferred by means of their computer systems. Nevertheless, an Internet service provider generally is required to take all reasonable steps to prevent further distribution of illegal material once aware of its nature.[155]

Dalam pencegahan dan penanggulangan *cybercrime* ini masing-masing pihak harus optimis, artinya kejahatan apapun yang dilakukan pasti ada jalan keluar untuk pencegahan dan penanggulangannya. Rasa optimis dalam diri **Michael A. Vatis** dalam penanggulangan *cybercrime* ini patut dicontoh seperti yang ia kemukakan dalam pernyataannya kepada Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommitte Washington D.C. sebagai berikut

> I am optimistic that the hard work of our agents, analysts, and computer scientists; the excellent cooperation and collaboration we have with private industry and universities; and the teamwork we are engaged in with foreign partners will in the end prove successful.[156]

---

154 Aedit Abdullah, *op.cit*. hal. 10

155 Dokumen PBB A.CONF.187/10 hal. 7

156 Michael A. Vatis, Statemen of the Record on *Cybercrime*, Februaty 29, 2000, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress02.htm

Rasa optimisme ini seperti ini tampaknya perlu ditumbuhkan pada setiap pengguna Internet, baik oleh kalangan politisi, pengusaha, budayawan, ilmuwan, dan terutama aparat penegak hukum. Bagi Polri rasa optimisme ini akan menumbuhkan semangat bahwa tidak ada kejahatan yang tidak bisa diberantas. Selalu saja ada jalan bagi orang-orang yang hendak menegakkan kebenaran dan keadilan dan selalu saja ada kekalahan bagi pelaku-pelaku kejahatan.

BAB IV

P E N U T U P

A. Kesimpulan

Kesimpulan yang dapat ditarik dari penelitian yang dilakukan adalah sebagai berikut :

1. *Hacking* (oleh *cracker*) dilakukan melalui beberapa tahap, yaitu
   a. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran;
   b. Menyusup atau mengakses jaringan komputer target sasaran;
   c. Menjelajahi sistem komputer (dan mencari akses yang lebih tinggi)
   d. Membuat *backdoor* dan menghilangkan jejak.

   Dari keempat tahap tersebut yang dapat dikonstruksikan sebagai kejahatan adalah tahap yang kedua sampai keempat. Tahap pertama tidak dapat dikonstruksikan sebagai kejahatan karena tahap ini hanya bersifat mempelajari atau belajar tentang sistem operasi komputer, belum ada aksi yang bersifat destruktif. Tahap kedua sampai keempat dikonstruksikan sebagai kejahatan karena pada tahap-tahap ini tindakan yang dilakukan *cracker* sudah dapat menimbulkan kerugian dan melanggar kepentingan pribadi dan/atau umum serta moral. Penetapan *hacking* sebagai kejahatan tidak hanya didasarkan pada sifat merugikan atau melanggar kepentingan pribadi dan/atau umum serta moral, tetapi mengingat Internet saat ini telah

digunakan untuk berbagai kegiatan, terutama kegiatan politik dan bisnis, maka penetapan atau pengkonstruksian *hacking* sebagai kejahatan tidak lepas dari kepentingan-kepentingan politik, ekonomi, sosial dan budaya yang ada dibaliknya.

2. Sampai saat ini di Indonesia terdapat sejumlah korban *hacking* yang jumlahnya tidak dapat dipastikan, karena para korban tidak mau melaporkan tindakan yang dilakukan oleh *cracker* terhadap situsnya ke polisi. Pada umumnya para korban merasa kesal, marah dan juga memandang apa yang dilakukan *cracker* sebagai kegiatan yang menganggu dan merugiakan kegiatan atau kerja mereka (baik yang situsnya digunakan untuk pelayanan umum maupun bisnis). Reaksi mereka terhadap aksi *cracker* itu menyebabkan munculnya stigma atau label pada *cracker* sebagai penjahat profesional atau disebut juga *white collar crime* khususnya kategori *professional occupational crime* karena kemampuan menguasai teknik *hacking* dan mempraktekkannya. Meskipun mereka telah bereaksi terhadap aksi *cracker* ini, tetapi belum ada *cracker* perusak situs yang dapat ditangkap atau diadili di Indonesia, hal ini menimbulkan kecemasan pada para korban khususnya dan pengguna internet (pemilik situs) pada umumnya. Jikapun ada pelaku *cybercrime* (dalam hal ini pelaku penyalahgunaan kartu kredit) yang ditangkap, itu bukan murni hasil usaha polisi tetapi berdasarkan laporan dari pihak lain. Melihat kondisi seperti ini para korban dan mereka yang belum menjadi korban mengambil langkah sendiri untuk menghadapi ancaman *cracker* di masa mendatang. Langkah tersebut berupa langkah

preventif berupa usaha-usaha untuk memperkuat sistem keamanan pada situsnya dan langkah *recovery* untuk memulihkan situsnya yang telah dirusak kemudian memasang sistem keamanan yang lebih kuat/baik,

3. Tidak ada perlindungan yang diberikan oleh pemerintah kepada para pemilik situs atau *website*, baik yang telah menjadi korban aksi *cracker* atau yang belum, meskipun memberi perlindungan kepada warganegara dan harta bendanya menjadi tanggung jawab negara/pemerintah. Negara/pemerintah tidak dapat memberi perlindungan kepada mereka berkaitan dengan dua hal, pertama belum adanya undang-undang yang mengatur kegiatan di *cyberspace*, khususnya yang menyangkut *cybercrime* dan kedua pihak kepolisian belum mempunyai kemampuan untuk menangani aksi *cracker* ini. Berbagai usaha untuk membei perlindungan kepada para pemilik situs atau *website* telah dilakukan oleh pemerintah, yaitu dengan dibuatnya perundang-undangan yang mengatur kegiatan di *cyberspace* dan meningkatkan kemampuan personil kepolisian baik dengan pelatihan (di dalam maupun luar negeri) dan bekerjasama dengan individu atau pihak swasta yang mempunyai komitmen untuk memberantas aksi *cracker* khususnya dan *cybercrime* pada umumnya.

B. Rekomendasi

Saran atau rekomendasi yang dapat diberikan penulis berikan berkaitan dengan hasil penelitian adalah sebagai berikut:

1. *Hacking* membawa keuntungan (terutama yang dilakukan oleh hacker sejati) dan kerugian (terutama yang dilakukan oleh cracekr ataupun bogus hacker). Tindakan yang merugikan dari hacking tidak hanya dipandang

dari sisi bisnis, tetapi juga dari sisi politis. Mengingat kerugian yang ditimbulkan oleh aksi cracker ini maka sudah saatnya *hacking* dikriminalisasikan. Kriminalisasi ini dilakukan untuk memberi perlindungan kepada pemilik situs atau *website* dan mencegah aksi *cracker* di masa yang akan datang karena aksi-aksi seperti itu akan semakin meningkat seiring dengan pemanfaatan dan pemasyarakatan Internet. Kriminalisasi ini perlu dilakukan untuk menyesuaikan diri dengan pergaulan internasional (berkaitan dengan hasil Kongres PBB X/2000) khususnya dalam usaha pencegahan *cybercrime* yang melintasi batas-batas negara.

2. Usaha kriminalisasi itu dapat dilakukan dengan menggunakan beberapa model. Model *umbrella provisions* dapat dipakai yang berarti *cyberlaw* merupakan hukum khusus yang hanya mengatur kegiatan di *cyberspace* termasuk masalah *cybercrime*. Model *triangle regulations* dapat juga dipakai yang berarti pada tiap-tiap peraturan yang mengatur berbagai kegiatan di *cyberspace* mengandung ketentuan pidana. Dapat juga digunakan metode penafsiran pada RUU KUHP dengan memperluas pengertian yang dapat mencakup *cybercrime* yang berarti untuk dua dunia yang berbeda, dunia nyata dan dunia maya, digunakan satu peraturan pidana. Untuk langkah yang terakhir ini perlu dipikirkan kemungkinan pengembangan peraturan pidana itu dengan amandemen mengingat perkembangan *cybercrime* yang sangat cepat.

DAFTAR PUSTAKA

A. Buku (Cetak dan Elektronik)

Aboba, Bernard, 1997, *The Online User's Encylopedia*, Addison-Wesley pada artikel *How the Internet Came Be*. versi elektronik dapat dijumpai di http://www.isoc. org/internet/history/vcerf.html, modifikasi terakhir 20 Juni;

Aoiki, Kumiko, 1994, *Virtual Communities in Japan*, paper at the Pacific Telecommunications Council Conference, versi elektronik dapat dijumpai di http://metalab.unc.edu/pub/academic/communications/papers/Virtual-Communities-in-Japan; dan http:// www.vcn.bc.ca/sig/comm-nets/aoki.txt

Arief, Barda Nawawi, 1998, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Citra Aditya Bakti, Bandung;

----------,1996, *Kebijakan Legislatif dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, BP UNDIP, Semarang;

----------, 1996, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung;

Atmasasmita, Romli, 1992, *Teori dan Kapita Selekta Kriminologi*, PT. Eresco, Bandung;

----------, 1984, *Bunga Rampai Kriminologi*, Rajawali Press, Jakarta;

----------, 1983, *Capita Selecta Kriminologi*, Armico, Bandung;

Badan Pembinaan Hukum Nasional, 1995/1996, *Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi*, BPHN Departemen Kehakiman R.I., Jakarta;

Barrett, Neill, 1997, *Digital Crime, Policing the Cybernation*, Kogan Page Ltd, London;

Beamish, Anne, 1995, *Communities On-line: Community-Based Computer Networks*, Thesis at the Massachusetts Institute of Technology, February; versi elektronik dapat dijumpai di http://sap.mit.edu/anneb/cn-thesis.html atau http://loohooloo.mit.edu/4.207/anneb/thesis/toc.html

Becker, D, *Research on Virtual Communities: an Empirical Approach*, versi elektronik dapat dijumpai di http://www.swipsy.uva.nl/usr/beckers/publication/scattle

Becker, Howard S., 1973, *Outsiders: Studies in the Sociology Deviance*, The Free Press, New York;

Bendikt, Michael (ed), 1991, *Cyberspace*, Cambridge, Mass: MIT Press;

Berger, Peter L., 1985, *Humanisme Sosiologi*, Inti Sarana Aksara, Jakarta;

---------- and Luckman, Thomas, 1990, *Tafsir Sosial Atas Kenyataan, Risalah Tentang Sosiologi Pengetahuan*, LP3ES, Jakarta;

----------, *Langit Suci, Agama Sebagai Realitas Sosial*, LP3ES, Jakarta, 1994;

Bertsch, Gary K. and Mclntrye, John R. (ed), 1983, *National Security and Technology Transfer: The Strategic Dimensious of East-West Trade*, Westview Press Inc, Colorado;

Brunvand, Eric, 1996, *The Heroic Hacker: Legends of the Computer Age*, modifikasi terakhir 15 Oktober, versi elektronik dapat dijumpai di http://www.cs.utah.cdu/ ~clb/nodc3.html;

Childress, James F., 1989, *Prioritas-prioritas Dalam Etika Biomedis*, Kanisius, Yogyakarta;

Chodwick, Bruce A. et.al., 1991, *Metode Penelitian Ilmu Sosial*, IKIP Semarang Press;

Clinard & Yeager, 1980, *Corporate Crime*, The Free Press A Division of Mac Millan Publishing Co. Inc, New York;

DeMelo, Diane M., *Criminology Theory on the Web*, dapat dijumpai di http://personal.tmlp.com /ddemelo/crime/;

Dirdjosisworo, Soedjono, 1995, *Pengantar Penelitian Kriminologi*, Ghalia Indonesia, Jakarta;

Dunning, Jhon H. (ed), 1971, *The Multinational Enterprise*, George Allen & Unwinn Ltd, London;

Faisal, Sanafiah, 1990, *Penelitian Kualitatif*, Dasar-dasar dan Aplikasi, Y A 3 Malang;

Fitzgerald, P.J. 1962, *Criminal Law and Punishment*, Clarendon Press, Oxford;

Frame, J. Davidson, 1984, *International Business and Global Technology*, DC Heat and Company, Lexington;

Gibson, William, 1984, *Neuromancer*, New York: Ace;

Hardy, Henry Edward, 1998, *The History of the Net*, versi elektronik dapat dijumpai di http://www.ocean.ic. net/ftp/doc/nethist.html, modifikasi terakhir April 02;

Hauben, Ronda, *The Development of the International Computer Network From Arpanet to Usenet News (On the Naurishment on Impediment of the Net_Commonwealth)*, Unpublished draft: Usenet Newsgroup news.admin.misch.article number 2577;

----------, *Netizens: On The History and Impact of The Net*, versi elektronik dapat dijumpai di http://www.columbia.edu/~rh120/ch_d13_rights.html

Herring, Susan (ed), *Computer-Mediated Communication: Linguistic, Social, and Cross-Cultural Perpective*, versi Electronik dapat dijumpai di http://www.sscnet.ucla.edu/soc/faculty/kollock/papers/vcommons.html;

Jacob, T., 1996, *Menuju Teknologi Berperikemanusiaan*, Yayasan Obor Indonesia, Jakarta;

----------, 1993, *Manusia, Ilmu dan Teknologi*, PT. Tiara Wacana, Yogyakarta;

Johnson, Doyle Paul, 1990, *Teori Sosiologi, Klasik dan Modern 2* (terjemahan Robert M.Z. Lawang), Gramedia, Jakarta;

Kartono, Kartini, 1983, *Patologi Sosial*, CV. Rajawali, Jakarta;

Kleinrock's, Leonard, 1996, *The Birth of the Internet*, pada Leonard Kleinrock's Personal History/Biography, versi elektronik dapat dijumpai di http://www.isoc.org/internet/ history/birth.html, modifikasi terakhir August 27;

Kollock, Peter dan Smith, Marc (ed), 1999, *Communities in Cyberspace*, London: Routledge, versi electronik dapat dijumpai di http://www.sscnet.ucla.edu/ soc/faculty/kollock/papers/communities_01.html

Kusumah, Mulyana W, 1991, *Aneka Permasalahan Dalam Ruang Lingkup Kriminologi*, Alumni, Bandung;

----------, 1984, *Kriminologi dan Masalah Kejahatan (Suatu Pengantar Ringkas)*, Armico, Bandung;

----------, 1982, *Realitas Sosial Kejahatan*, Prisma, LP3ES, Jakarta, 5 Mei 1991, *Aneka Permasalahan Dalam Ruang Lingkup Kriminologi*, Alumni, Bandung;

Lapham, Lewis H (ed), 1989, *Teknologi Canggih dan Kebebasan Manusia*, Yayasan Obor, Jakarta;

Latifulhayat, Atip, 2000, *Legal Protection of Databases And Its Implications For Indonesian Law Relating to Intellectual Property Rights*, Thesis in Monash University, Australia;

Legion of the Underground, *Hacking Guide*, versi elektronik dapat dijumpai di http://www.geocities. com/dht_belgium/lou_guide.txt;

Leiner, Barry M, et.al., 2000, *A Brief History of the Internet (English version)*, versi elektronik dapat dijumpai di http://www.isoc.org/internet/history/ brief.html, modifikasi terakhir August 4;

Lipnack, Jessica & Stamps, Jeffrey, 1994, *The Age of The Network, Organizing Principles for the 21st Century*, John Wiley & Sons, Inc.;

Levin, James, et.al., 1980, *Criminal Justice A Public Policy Approach*, Harcourt Brace Jovanovich, New York;

Miles, Matthew b & Huberman, A. Michael, 1995, *Analisa Data Kualitatif*, UI Press, Jakarta;

Mistry, Shailen S., *Hacker on the Net*, versi elektronik dapat dijumpai http://lis.gseis.ucla.edu/ impact/196/Projects/Smistry/index.html;

Moleong, Lexy J, 1995, *Metodologi Penelitian Kualitatif*, Remaja Rosdakarya, Bandung;

Muladi dan Arief, Barda Nawawi, 1992, *Bunga Rampai Hukum Pidana*, Alumni, Bandung;

--------, 1990, *Proyeksi Hukum Pidana Materiil Indonesia di Masa Mendatang*, Pidato Pengukuhan Guru Besar Universitas Diponegoro, Semarang;

Muraskin, Roslyn & Roberts, Albert R., 1996, *Vision For Change - Crime and Justice and in the Twenty-First Century*, Prentice-Hall Inc, A Simon & Schuster Company Upper Saddle River, New Jersey;

Naisbitt, John; Naisbitt, Nana and Philips, Douglas, 2001, *High Tech High Touch, Pencarian Makna Di Tengah Perkembangan Pesat Teknologi*, Mizan, Bandung;

Negroponte, Nicholas, 1998, *Being Digital, Menyiasati Hidup Dalam Cengkeraman Sistem Komputer*, Mizan, Bandung;

Noach, W.M.E. dan van den Heuval, Grat, 1992, *Kriminologi Suatu Pengantar* (terjemahan J.E. Sahetapy), Citra Aditya Bakti, Bandung;

Nonet, Phillip & Selznick, Philip, 1978, *Law and Society In Transition, Toward Responsive Law*, Harper and Row, New York;

Nur, Muhammad, 1998, *Beberapa Gagasan Untuk Kemajuan Teknologi Menuju Pada Kemandirian Sains*, Pidato Dies Natalis ke 41 UNDIP Semarang, 15 Oktober;

Ohmae, Kenichi, 1991, *Dunia Tanpa Batas, Kekuatan dan Strategi Di Dalam Ekonomi yang Saling Mengait*, Binarupa Aksara, Jakarta;

Poloma, Margaret M, 1994, *Sosiologi Kontemporer*, RajaGrafindo Persada, Jakarta;

Prana, Gede Artha Azriadi, 1999, *Hacker, Sisi Lain Legenda Komputer*, Adigna, Jakarta;

Purbo, Onno W. dan Wahyudi, Aang Arif, 2001, *Mengenal eCommerce*, Elex Media Komputindo, Jakarta;

----------, dan Wiharjito, Tony, 2000, *Keamanan Jaringan Internet*, Elex Media Komputindo, Jakarta;

----------, et.all, 1998, *TCP/IP, Standar, Desain dan Implementasi*, Elex Media Komputindo, Jakarta;

Quinney, Richard, 1980, *Class, State and Crime*, Longman Inc, New York;

----------, 1975, *Criminology: Analysis and Critique of Crime in America*, Brown and Co. Inc, New York;

Radzinowicz, Leon, 1966, *Ideology and Crime, A Study of Crime in its Social and Historical Context*, Heinemann Educational Books, London;

Rahardjo, Budi, 2000, *Keamanan Sistem Informasi Berbasis Internet*, PT. Insan Komunikasi/Infonesia-Bandung, versi elektronik dapat dijumpai di http://budi.insan.co.id/book/handbook.pdf.;

Raillon, Francois, 1990, *Indonesia Tahun 2000 (Tantangan Teknologi dan Industri)*, (terjemahan Nasir Tamara), CV. Haji Masagung, Jakarta;

Rasch, Mark D., 1996, *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, Computer Law Association; versi elektronik dapat dijumpai di http://cla.org/RuhBook/chp11.htm;

Raymond, Eric, 1994, *The New Hacker's Dictionary*, MIT Press; http://www-mitpress.mit.edu/scb/book-homc/0262680920.htm;

----------, 2000, *How To Become A Hacker*, edisi revisi 1.92, September, versi elektronik dapat dijumpai di http://www.tuxedo.org/~esr/faqs/hacker-howto.html;

Reddick, Randy & King Elliot, 1996, *Internet untuk Wartawan, Internet Untuk Semua Orang*, Yayasan Obor, Jakarta;

Rheingold, Howard, 1991, *Virtual Reality*, Mandarin, versi electronic dapat dijumpai di http://www.rheingold.com/vc/book/intro.html

Reksodipuro, Mardjono, 1994, *Kriminologi dan Sistem Peradilan Pidana*, Lembaga Kriminologi UI, Jakarta;

Ritzer, George, 1985, *Sosiologi, Ilmu Pengetahuan Berparadigma Ganda* (penyadur: Alimandan), Rajawali, Jakarta;

Rosenoer, Jonathan, 1997, *Cyberlaw, The Law of the Internet*, Spring-Verlag, New York;

Sahetapy, J.E., 1992, *Teori Kriminologi*, Citra Aditya Bakti, Bandung;

----------, dan Reksodiputro, B. Mardjono, 1983, *Paradoks Dalam Kriminologi*, CV. Rajawali, Jakarta;

----------, 1984, *Pisau Analisa Kriminologi*, Pidato Pengukuhan Guru Besar di UNAIR Surabaya, 30 Juli 1983, Armico, Bandung;

Slouka, Mark, 1999, *Ruang yang Hilang, Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan*, Mizan, Bandung;

Smith, J.C. and Hogan, Brian, 1988, *Criminal Law*, English Language Book Society/Butterworths, London;

Soekanto, Soerjono; Liklikuwata, Hengki dan Kusuma Mulyana W., 1986, *Kriminologi, Suatu Pengantar*, Ghalia Indonesia, Jakarta;

Soemitro, Ronny Hanitijo, 1994, *Metode Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta;

----------, 1990, *Hukum dan Perkembangan Ilmu Pengetahuan dan Teknologi di Dalam Masyarakat*, Pidato Pengukuhan pada Upacara Peresmian Penerimaan Jabatan Guru Besar Tetap pada Fakultas Hukum UNDIP, Semarang, 6 Desember;

Stallings, William, 1995, *Network and Internetwork Security*, Prentice Hall; New Jersey;

Sterling, Bruce, 1990, *The Hacker Crackdown, Law and Disorder on the Electronic Frontier*, Massmarket Paperback, 1990 http://www.lysator.Liu.se/etexts/hacker/;

Sudarto, 1986, *Hukum dan Hukum Pidana*, Alumni, Bandung;

Suheimi, 1991, *Kejahatan Komputer*, Andi Offset, Yogyakarta;

Suler, John, 1999, *The Psychological of Cyberspace, Overview and Guided Tour*, September, versi elektronik dapat dijumpai di http://www.rider.edu/users/suler/psycyber/psycyber.html

Sumardjono, Maria SW, 1996, *Pedoman Pembuatan Usulan Penelitian, Sebuah Panduan Dasar*, Gramedia, Jakarta;

Suparno, Paul, 2001, *Filsafat Konstruktivisme Dalam Pendidikan*, Kanisius, Yogyakarta;

Susanto, I.S., 1995, *Diktat Kriminologi*, FH UNDIP, Semarang;

----------, 1995, *Kejahatan Korporasi*, BP UNDIP, Semarang;

----------, 1990, *Statistik Kriminal Sebagai Konstruksi Sosial (Penyusunan, Penggunaan dan Penyebarannya, Suatu Studi Kriminologi)*, Ringkasan Disertasi untuk memperoleh Gelar Doktor dalam Ilmu Hukum di UNDIP Semarang, 10 Maret;

Sutopo, Heribertus, 1998, *Pengantar Penelitian Kualitatif, Dasar-dasar Teoritis dan Praktis*, Pusat Penelitian UNS, Surakarta;

Taylor, Ian; Walton, Paul; Young, Jack; 1973, *The New Criminologi for a Social Theory of Deviance*, International Library of Sociology, edited by John Rex, Routledge and Kegan Paul, London & Boston;

The Mentor, 1989, *A Novice's Guide to Hacking*, versi elektronik dapat dijumpai di http://www.geocities.com/dlit_belgium/Legion_of_Doom.txt;

Tim Redaksi Driyarkara, 1993, *Seri Filsafat Driyarkara: 6 Capita Selecta Diskursus Kemasyarakatan dan Kemanusiaan*, Gramedia, Jakarta;

Veeger, K.J., 1986, *Realitas Sosial, Refleksi Filsafat Sosial atas Hubungan Individu-Masyarakat dalam Cakrawala Sejarah Sosiologi*, Gramedia, Jakarta;

Wang, Zheng, 1997, *The Early Pioneers*, versi elektronik dapat dijumpai di http://www.bell-labs.com/user/zhwang/hist.html, modifikasi terakhir, June 20;

Wisnubroto, Al., 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Penanggulangan Kejahatan Komputer*, Atmajaya Press University, Yogyakarta;

Zakon, Robert H'obbes', 1995, *Hobbes' Internet Timeline v5.1.*, versi elektronik dapat dijumpai di http:// www.isoc.org/quest/zakon/internet/history/HIT.html. publikasi terakhir October 16;.

Zaleski, Jeff, 1999, *Spiritualitas Cyberspace, Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*, Mizan, Bandung;

Zeviar-Geese, Bagriola, *The State of the Law on Cyberjurisdiction and Cybercrime on the Internet*, versi elektronik dapat dijumpai di http://www.law.gonzaga.edu/border... yberlaw.htm;

Widodo, Dian, 1996, *Kamus Jaringan Komputer, Dilengkapi dengan Daftar Akronim dan Daftar Alamat E-Mail*, Andi, Yoygakarta;

Williams III, Frank P. and McShane, Marilyn D., 1988, *Criminological Theory*, Englewood Cliffs, New Jersey, Prentice Hall;

B. Makalah dan Artikel

Abdullah, Aedit, 2001, *Cybercrime in Singapore (and Money-Laundering)*, Makalah pada Seminar Nasional Money Laundering dan *Cyber* Crime dalam Perspektif Penegakan Hukum di Indonesia, Lab Hukum Pidana, FH Univ. Surabaya, 24 Februari;

Ahmad, Ismail, 2000, *Regulasi Voice over Internet Protocol*, Makalah pada Seminar Teknologi 2k dengan tema VoIP Dalam Rangka Dies Natalis XVII Teknik Elektro UNDIP, Semarang, 14 Desember;

Andoko, Andrey, 2000 *Bill Gates Tokoh yang Dipuji dan Dimaki*, Kompas, 28 Juni;

Arief, Barda Nawawi, 2001, *Kebijakan Kriminalisasi dan Masalah Yuridis Tindak Pidana Mayantara*, Makalah pada Seminar Nasional RUU Teknologi Informasi (Cyberlaw) dengan tema Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi, Kerjasama Ditjen Postel Departemen Perhubungan dengan FH UNDIP Semarang, 26 Juli;

----------, 2001, *Antisipasi Penanggulangan Cyber Crime Dengan Hukum Pidana*, Makalah pada Seminar Nasional Cyberlaw, diselenggarakan STH Bandung, 9 April;

Barlow, John Perry, 1996, *A Declaration of the Independece of Cyberspace*, Davos, Switzerland, February 8, versi elektronik dapat dijumpai di http://www.eff.org/~barlow;

Brill, Charles, 1998, *Legal Protection of Collections of Facts*, Computer Law Review and Technology Journal, Spring;

Budjijanto, Danrivanto, 2000, *Aspek-aspek Hukum Dalam Perniagaan Secara Elektronik (E-Commerce)*, Makalah pada Seminar Nasional Aspek Hukum Transaksi Perdagangan via Internet di Indonesia (E-Commerce) di selenggarakan FH UNPAD, Bandung, 22 Juli;

Cailliau, Robert, 1995, *A Short History of the Web*, WebCore Dissemination, IW3C2, Paris, 2 November, versi elektronik dapat dijumpai di http://www.inria.fr/Actualitas/ Cailliau-fra.html;

Chandra, Fransisca Haryanti, 1995, *Internet: Information Superhighway*, Makalah pada Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer bagi Dosen PTS Kopertis Wilayah VI di Semarang, 4 - 8 September;

Cerf, Vint, 1995, *IETF and ISOC*, dapat dijumpai di http://www.isoc.org/internet/ history/ietfhis.html, modifikasi terakhir 16 Oktober;

Donoseputro, Marsetio, 1991, *Pendidikan, Iptek dan Pembangunan*, Surabaya Post, 3 Agustus;

Dari Cambridge Menuju Kopenhagen, Seri Penerbitan Sains, Teknologi dan Masyarakat, Edisi I, Mizan, Bandung, 2000;

Freeh, Louis J. , 2000, *Statemen of the Record on Cybercrime*, Februaty 16, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress03.htm;

Gallagher, Neil J., 1999, *Statemen of the Record on Cybercrime, Transnational Crime, and Intellectual Property*, March 24, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress08.htm;

Gore, Al, 1993, *Speech at the Superhighway Summit Royce Hall*, January 11, UCLA Los Angeles, California, versi electronik dapat dijumpai di http://www.cff.org/pub/GII_NII/Govt_docs/gore_shs.speech;

----------, 1996, *Bringing Information to the World: The Global Information Infrastructure*, Harvard Journal of Law & Technology 1, Winter 1996;

Hagan, Jhon, 1994, *Studying Criminology, Why Criminology*? Dalam Modern Criminology, Crime, Criminal Behaviour and Its Control, diterjemahkan Mufid menjadi *Mengenal Kriminologi*, Majalah Legality, Vol. 3/II/Maret-Agustus;

Handoko, Yus Dwi, 2000, *Membuat Mailing List di eGroups*, dalam majalah Internet, Edisi 15 November - 15 Desember;

----------, 2000, *Mencari File di Internet*, Majalah Internet, Edisi 15 November-15 Desember;

----------, 2000, *Memanfaatkan Program Telnet*, Majalah Infokomputer Vol. XIV No. 02 Februari;

Harahap, Khrisna, 2001, *Kebebasan Pers Di Indonesia Memasuki Cyber Communication*, Makalah pada Seminar Nasional mengenai *Cyberlaw*,

diselenggarakan oleh Sekolah Tinggi Hukum Bandung (STHB) di Bandung, 9 April;

Hartono, Sunaryati, 1981, *Pembahasan Kerta Kerja: Pemindahan Teknologi dan Pengaturannya dalan Peraturan Perundang-undangan*; dalam Seminar Aspek-aspek Hukum Pengalihan Teknologi, dipublikasikan oleh Badan Pembinaan Hukum Nasional, Binacipta, Bandung;

Hendarman, Rudi, 1995, *Computer Fraud*, Majalah Pro Justitia UNPAR, Tahun XIII No. 2 April;

Irawan, FX. Bambang, *Logika Boolean Efektifkan Pencarian*, Tabloid PCplus o. 12/11/10-16 Januari 2001

Katsh, M. Ethan, Oktober 1995, *Cybertime, Cyberspace and Cyberlaw*, Journal of Online Law, Collefe of Willian and Mary School of Law, June;

Kairandy, Ridwan, 1997, *Francise dan Kaitannya Sebagai Sarana Alih Teknologi: Suatu Tinjauan Hukum*, Jurnal Hukum Ius Quia Iustum FH UII Yogyakarta, No. 7 Vol. 4;

Kantaatmaja, Mieke Komar, 2000, *Meyongsong Penyusunan Peraturan Perundang-undangan Telematika (Cyberlaw)*, Makalah pada Seminar Nasional tentang Aspek Hukum Transaksi Perdagangan via Internet di Indonesia (E-Commerce) diselenggarakan oleh SEMA FH Unpad, Bandung, 22 Juli;

Kapor, Mitchell, 1991, *Civil Liberties in Cyberspace: When does Hacking Turn From an Exercise of Civil Liberties into Crime?* Scientific American, September;

Kelly, Michael, 1993, *David Gergen, Master of the Game*, New York Times, October 31;

Kollock, Peter and Smith, Marc, Managing the Virtual Commons: Cooperation and Conflict in Computer Comunities, dapat dijumpai di http://www.sscnet.ucla.edu/soc/faculty/kollock/papers/vccommons.html

Konstantinou, Jeanie, 1995, *Computer Hackers: Invasion of Computer System*, Computer and the Law Homepage, Dec. 8;

Latifulhayat, Atip, 2000, *Cyberlaw dan Urgensinya Bagi Indonesia*, Makalah pada Seminar tentang *Cyber* Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli;

Lubis, T. Mulya, 1987; *Alih Teknologi: Antara Harapan dan Kenyataan*, Prisma, No. 4 Th. XVI, April 1987;

Mahayana, Dimitri, 2001, *IT Application in Convergence Age*, Makalah pada Seminar Nasional RUU Teknologi Informasi (Cyberlaw) dengan tema Pemberdayaan Teknologi Informasi dalam Masyarakat Informasi, Kerjasama Ditjen Postel Departemen Perhubungan dengan FH UNDIP Semarang, 26 Juli

Mahendra, Yusril Ihza, 2000, *Regulasi Cyberspace Di Indonesia*, Makalah pada Seminar tentang *Cyber* Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli;

Makarim, Edmon, 2000, *Telematics Law, Cyberlaw, Media, Communication & Information Technologies*, Makalah pada Seminar tentang Cyber Law, diselenggarkan Yayasan Cipta Bangsa di Bandung, 29 Juli;

Manap, Nazura Abdul, 2001, *Cyber*-crimes: *Problems and Solutions Under Malaysian Law*, Makalah pada Seminar Nasional Money Laundering dan *Cybercrime* dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Lab. Hukum Pidana FH Univ. Surabaya, 24 Februari;

Miller, JoAnn L., 1994, *White Collar Crime*, Jurnal Ilmu-Ilmu Sosial 5 (Kejahatan Kerah Putih), PAU IS UI dan PT. Gramedia Pustaka Utama, Jakarta, Januari;

Moceyunas, Ann K., 1999, *On-line Privacy: the Push and Pull of Self-Regulation and Law*, Net Law News, Oct-Nov-Dec;

----------, 1999, *Computer Hacking: A New Warfare*, Net Law News, Oct-Nov-Dec;

Muladi, 2001, *Prosepek Pengaturan Cybercrime di Indonesia*, Makalah pada Seminar Nasional Money Laundering dan *Cybercrime* dalam Perspektif Penegakan Hukum di Indonesia, diselenggarakan oleh Lab. Hukum Pidana FH Univ. Surabaya, 24 Februari;

Nitibaskara, Ronny R, 2000, *Problem Yuridis Cybercrime*, Makalah pada Seminar Sehari Cyberlaw 2000, Bandung, 29 Juli, dapat juga dibaca di Kompas, edisi tanggal 29 dan 31 Juli;

Piliang, Yasraf Amir, 2000, *Mesin-mesin Kepalsuan*, Kompas, 14 Juni, versi elektronik dapat diperoleh di http://www.kompas.com/mesi45;

----------, 1998, *Hiper Kriminalitas*, Kompas, 30 Oktober, versi elektronik dapat dijumpai di http://www.kompas.com/hipe04.htm

Prakoso, Samuel, 2001, *Mengenal HTML*, Buletin Jendela Informatika, vol 2 No. 1;

Purbo, Onno W., 2001, *Cyberlaw: Filosofi "Hukum" Di Dunia Maya*, Makalah pada Seminar Nasional Cyberlaw, diselenggarakan oleh STH Bandung, 9 April;

----------,2000, *Perkembangan Teknologi Informasi dan Internet di Indonesia*, Kompas, 28 Juni;

----------, 1997, *Diskusi Melalui Mailing List Di Internet*, Infokomputer Edisi Internet, Vol. I No. 4, Mei-Juni;

----------, 1996, *Internet Untuk Seluruh Universitas Di Indonesia: Visi Sebuah Teknologi Merakyat*, Makalah pada Seminar Pengenalan dan Pemanfaatan Internet, Purwokerto, 15 Juni;

Purwadi, Ari, 1993, *Kebutuhan Akan Perangkat Hukum Perjanjian Di Bidang Alih Teknologi*, Hukum dan Pembangunan, No. 3 Th. XXIII Juni 1993;

Rasyid, Rafdian, 2000, *Membongkar Rahasia ISP Anda*, dalam Infokomputer, Februari;

Rahardjo, Budi, 2000, *Implikasi Teknologi dan Internet Terhadap Pendidikan, Bisnis dan Pemerintahan, Siapkah Indonesia?*, Makalah pada seminar di Riau, dapat dijumpai di http://budi.insan.co.id/articles/riau-it.doc;

Rahardjo, Satjipto, *Hukum Itu Tidak Steril*, Suara Pembaruan, 3 Agustus 1989;

Sahetapy, J.E., 1994, *White Collar Crime, Sebuah Perspektif Viktimologi*, Jurnal Ilmu-Ilmu Sosial 5 (Kejahatan Kerah Putih), PAU IS UI dan PT. Gramedia Pustaka Utama, Jakarta, Januari;

Samadikun, Samaun, 2000, *Pengaruh Perpaduan Teknologi Komputer, Telekomunikasi dan Informasi*, Kompas, 28 Juni;

Sasmojo, Saswinadi dan Yuliar, Sonny, *Budaya Sains, Teknologi dan Perubahan Masyarakat*, Seri Penerbitan Sains, Teknologi dan Masyarakat, Edisi I;

Satriananta, Ary, *Internet Telephony, A Broader Business Perspective of Delivering Telephony Service over Internet*, Makalah pada Seminar Teknologi 2k dengan tema VoIP Dalam Rangka Dies Natalis XVII Teknik Elektro UNDIP, Semarang, 14 Desember;

Scalione, Robert, 1996, *Crime in the Internet: Can the Law Keep Up With a New Generation of Cyberspace Hackers*, Computer and Law Homepage, Fall

Sianipar, Pandapotan, 2000, *Mencari Informasi dengan Fasilitas Search IE*, Majalah Internet, Edisi 15 November-15 Desember;

Silalahi, H. Daud, 1987, *Rencana Undang-undang Alih Teknologi: Perbandingan Perspektif*, Prisma, No. 4 Th. XVI, April;

Siregar, Ashadi, 2000, *Membaca Surat Kabar Digital, Membaca Wajah Populis Teknologi Media*, Kompas, 28 Juni

Soemitro, Ronny Hanitijo, 1993, *Grounded Research Dalam Penelitian Ilmu-ilmu Sosial*, Majalah Masalah-masalah Hukum No. 9;

Soerya, Rendra T., 2001, *Siapa Perlu Belajar Pemrograman*?, PCplus No. 15/II/06 Februari;

Sudarsono, Juwono, 1992, *Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial-Politik*, Masyarakat: Jurnal Sosialogi, FISIP UI-Gramedia, Jakarta;

Susanto, I.S., 1998, *Perkembangan Kriminologi*, Makalah Pada Penataran Nasional Hukum Pidana dan Kriminologi, Semarang, 23-30 November;

----------, 1997, *Menciptakan Lingkungan Hidup Yang Nyaman*, Pidato Dies Natalis UNDIP ke 40, 15 Oktober;

----------, 1992, *Pemahaman Kritis Terhadap Realitas Sosial*, Makalah pada Lokakarya Nasional Untuk Pengembangan Sumberdaya IMKA di Karangpandan, 12-17 Agustus;

Sutoyo, Johanes dan Meliala, Adrianus, *Politik Kejahatan Terhadap Pelaku White Collar Crime*, Jurnal Ilmu-ilmu Sosial, PAU IS UI dan Gramedia, Jakarta, Januari 1994;

The Growth and Development of Cyberspace Law in the United States: Highlights of the Past Decade, The UCLA Online Institute for Cyberspace Law dan Policy;

The Mentor, *The Consciensce of a Hacker*, Phrack vol 1 Edisi 7, file 3, versi Indonesia di http://www.k-elektronik.org/manifesto.html;

Tim DSM STIKOM Surabaya, 1997, *Pengantar HTML*, Infokomputer edisi Internet, Vol. 1 No. 6 Edisi 15 Juli-15 Agustus;

Weiner, Jon, 1994, *Statit in Cyberspace*, Article on The Nation Magazine, 1994, versi elektronik dapat dijumpai di http://www.igc.apc.org;

Widayadi, Didi, 2000, *Kebijakan dan Strategi Operasional POLRI Dalam Kaitan Hakekat Ancaman Cybercrime*, Makalah pada Seminar tentang *Cyber* Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli;

Wirahadikusumah, Miftah, 1992, *Logika dan Gramar Teknologi: Sebuah Tinjauan Psikoanalisis*, Masyarakat: Jurnal Sosiologi, FISIP UI-Gramedia, Jakarta;

Yuliantoro, Joko dan Purbo, Onno W., 1997, *PGP Sebagai Pengaman E-mail Anda*, dalam Majalah Infokomputer, Edisi Internet, Vol. 1 No. 4, 15 Mei-15 Juni;

Zaroni, 1996, *Menjadi Anggota Masyarakat Virtual Bersama Wasantara-Net, Presentasi dan Demo Internet*, Makalah pada Seminra Pengenalan dan Pemanfaatan Internet, Purwokerto, 15 Juni;

Vatis, Michael A., 2000, *Statement of The Record on The National Infrastructure Protection Center*, March 1, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress01.htm

----------, 2000, Statemen of the Record on *Cybercrime*, Februaty 29, versi elektronik dapat dijumpai di http://www.fbi.gov/pressrm/congress02.htm.

Wakefield, Mark, *Richard Quinney*, dapat dijumpai di http://www.criminology.tsv.edu/crimetheory/quinney.html

Who is this Guy who Calls Himself Hacker One, versi elektronik dapat dijumpai di http://www.im.lcs.mit.edu/gilliam/hacker-one.html;

C. Perundang-undangan dan Dokumen Lainnya (Cetak maupun Elektronik)

A Declaration of Independence of Cyberspace, http://www.eff.org/~barlow

Draft 27 of Convention on Cyber-crime and Explantory Memorandum, May 25, 2001. http://conventions.coe.int/treaty/en/projects/*cybercrime27*.doc

Draft 25 of Convention on Cyber-crime, December 22, 2000. http://conventions.coe.int/treaty/en/projects/*cybercrime25*.htm

Draft 24(2) of Convention on Cyber-crime, November 19, 2000. http://conventions.coe.int/treaty/en/projects/*cybercrime24*.htm

Draft 22 of Convention on Cyber-crime, October 2, 2000. http://conventions.coe.int/treaty/en/projects/*cybercrime22.doc*

Draft 19 of Convention on Cyber-crime, April, 2000, http://conventions.coe.int/treaty/en/projects/*cybercrime*.htm

Draft I RUU Teknologi Informasi disusun oleh FH UNPAD bekerja sama dengan Ditjen Pos dan Telekomunikasi, 2001;

European Union, Article 29 Working Group Opinion 4/2001, On the Council of Europe's Draft Convention on Cyber-crime, 22 March 2001. http://conventions.coe.int/a29 opinion301.pdf

Explanatory Memorandum, June 22, 2001. http://conventions.coe.int/treaty/en/projects/*cybercrimememmo-final*.htm

Final version of Convention on Cyber-crime, June 22, 2001. http://conventions.coe.int/treaty/en/projects/*cybercrime-final.*.htm

Kitab Undang-undang Hukum Pidana (KUHP)

Naskah Akademik Rancangan Undang-undang Tentang Teknologi Informasi, Prakarsa Direktorat Jenderal Pos dan Telekomunikasi, Departemen Perhubungan RI dengan FH UNPAD Bandung, 2000;

TAP MPR No. IV/MPR/1973 tentang GBHN

TAP MPR No. IV/MPR/1978 tentang GBHN

TAP MPR No. II/MPR/1983 tentang GBHN

TAP MPR No. II/MPR/1993 tentang GBHN

The Children's Online Privacy Protection Act 1998

The Computer Misuse Act 1998 (Singapura)

The Information Technology Act 1999 (India), http://www.cyberlawindia.com/itbill.html

The Computer Crime Act 1997 (Malaysia)

Undang-undang No. 39 Tahun 1999 tentang Hak Asasi Manusia;

United Nation, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, *Crimes related to computer networks,* Vienna, 10-17 April 2000;

United Nation, Forth United Nations Congress on the Prevention of Crime and the Treatment of Offender

WIPO Licencing Guide for Developing Countries, Geneva, 1977

D. Kamus

Kamus Istilah Internet, Kerjasama Wahana Komputer Semarang dengan Penerbit Andi Yogyakarta, 2000

The New Hacker's Dictionary, MIT Press, 1994

The Pocker Oxford Dictionary, YMCA Library Building, Jai Singh Road, New Delhi, 1996

E. Majalah/Koran/Tabloid/Lain-lain

Associated Press, February 15, 2000

Infokomputer Vol. XI No. 8 Agustus 1995

Infokomputer, Edisi Khusus Internet, Vol. I/3, 15 April-15 Mei 1997

Info Komputer, Volume XI No. 5 Mei 1997

Infokomputer, Edisi Internet Vol. 1 No. 4, 15 Mei-15 Juni 1997

Infokomputer, Edisi Internet, Juli-Agustus 1997

Info Komputer, Volume XII No. 8 Agustus 1998

Jawa Pos, 1 Oktober 2000,

Kompas, 23 Juli 2000

Kompas, 1 Desember 1999

Kompas, 23 Juli 2000

Media Indonesia, 2 September 2000

Republika, 17 Februari 2000

Republika, 22 Agustus 1999

Republika 26 September 1999

Republika, 16 Januari 2000

Reuters, February 15, 2000

Suara Merdeka, 17 November 2000

Suara Pembaruan, 22 Juli 2000

Tabloid Komputer PCplus, No. 12/II/10-16 Januari 2001
Tabloid Komputer PCplus No. 15/II/31 Januari-06 Februari 2001
Tabloid Komputer PCplus No. 16/II/7-13 Februari 2001
Tabloid Komputer PCplus No. 18/II/21-27 Februari 2001
Tabloid Komputer PCplus No. 20/II/07-13 Maret 2001